Europäisches Patentamt	European Patent Office	Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03005263.3

CERTIFIED COPY OF PRIORITY DOCUMENT

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

BEST AVAILABLE COPY

Anmeldung Nr:
Application no.: 03005263.3
Demande no:

Anmeldetag:
Date of filing: 10.03.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Sony International (Europe) GmbH
Kemperplatz 1
10785 Berlin
ALLEMAGNE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

A method for handover in internet protocol and cellular telecommunications network

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L29/06

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI SK TR LI

EPO - Munich
50
10. März 2003

The invention generally relates to mobile computing in an ad hoc networking environment. More specifically, it is directed to the field of Quality-of-Service (QoS) management for adaptive real-time services running on mobile devices which support different access technologies in dynamic ad hoc Internet Protocol (IP) networks, where the connectivity of the applied nodes is unpredictable time-varying.

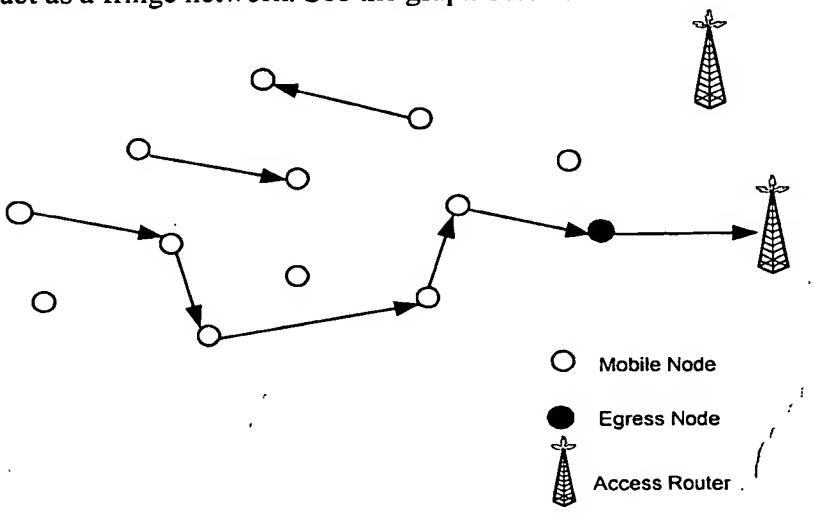
In this context, the invention presents methods for a QoS aware handover with resource probing, pre-allocating, reserving, and adapting in a dynamic ad hoc environment.

EPO - Munich
50
10. März 2003

MAC-IP Address Mapping Implementation (MIAMI)

1. MANET

A "mobile ad hoc network" (MANET) is an autonomous system of MNs connected by wireless links--the union of which form an arbitrary graph. Each mobile node operates not only as an end-system, but also as a router to forward packets. These "routers" in MANET are free to move randomly and organize themselves arbitrarily; thus, the whole network's wireless topology may change rapidly and unpredictably. This is in contrast with the topology of the existing Internet, where the topology is essentially static. Such a network may operate in a standalone fashion, or may be connected to the larger Internet, act as a fringe network. See the graph below.



MANET has some special characteristics:

- Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology, which is typically multi-hop, may change randomly and rapidly at unpredictable times. Adjustment of transmission and reception parameters such as power may also impact the topology.

- Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently.

- Power-constrained operation: Some or all the nodes in a MANET may rely on batteries for their energy. For these nodes, the most important system design criteria for optimization may be that of power conservation.

- Limited physical security: Mobile wireless networks are generally more prone to physical security threats than fixed networks. Existing link security techniques are often applied within wireless networks to reduce security threats.

2. Existing Approaches for Address Resolution

2.1 ARP in IPv4

ARP is the most useful protocol in IPv4. It is useful in a broadcast medium, like Ethernet. ARP uses flooding packets. Every host has a small cache to save mapping information, and all hosts are equal in status, no distinction between clients and servers.

2.2 Reverse ARP (RARP)

RARP is also used in broadcast medium with flooding packets, like ARP. The difference is that, RARP needs one or more server hosts, to maintain a database of mapping information, and to respond to requests from client hosts.

Most implementations of RARP will require some form of interaction with a program outside of the kernel. RARP separates protocol at the data-link level, it is independent of medium, and can be used for mapping hardware addresses to any higher level protocol address. On this point it is different from ARP.

2.3 IPv6 Neighbor Discovery Protocol (ND)

IPv6 ND extends and improves on IPv4's ARP, it is embedded within ICMPv6, and defining new functionality, e.g., Neighbor Unreachability Detection.

To perform ND, the node needs to have multicast-capable interface(s), and it performs only on addresses that are determined to be on-link, never on multicast addresses. Furthermore, unsolicited node doesn't need to create an entry in the cache when receiving a valid Neighbor Advertisement.

2.4 Inverse Neighbor Discovery Protocol (IND)

IPv6 IND is the extension to IPv6 ND. It is initially developed for Frame Relay networks, or networks with similar behavior. IND Solicitation is sent as IPv6 all-node multicast. However at link layer, it is sent directly to the target node, a directly connected remote node identified by the known link-layer address.

3. Basic Idea of MAC-IP Address Mapping

The proposed protocol "MIAMI" is "Proactive". The initial MN proactively adds its own mapping information and some other possible known mapping information in the hop-by-hop options headers of normal IP packets, sends IP traffic to other MNs along the route. The MNs on the path can save or update the information locally and proactively change and forward the header.

In this way, the MAC-IP mapping information can be spread out, from spot to line, from line to area. At the first stage, the mapping information could be located in several isolate "regions" among the mobile ad hoc fringe. When there are more and more MNs involved, and more and more IP traffics, the regions could be united together, forming larger

regions, and finally build up a "distributed, dynamic" mapping information database. The database forms smoothly. This scenario looks like the oil spots splashed down on the surface of the water merge together and finally form a whole oil area.

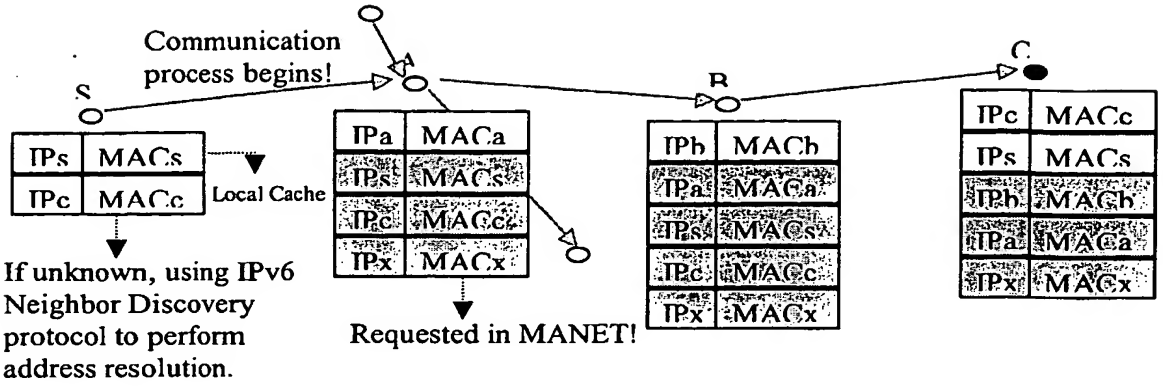
3. Detail discuss

Firstly, we define one constant parameter "MAX_HOP", which indicates the maximum hops that the mapping information should be transferred along the traffic path. The value can be adjusted according to the network context of the mobile ad hoc fringe. For the large fringe, it could be 3, for smaller, it could be 1 or 2. We don't adapt this value according to the different L2 access technologies, because of the following reasons. First, the protocol should not depend on any special access technologies; second, for example, two neighboring nodes, the former node using access technology A, prefers MAX_HOP as 3; the later node using access technology B, prefers MAX_HOP as smaller value, 1. Then, the mapping information of the former node will not be spread as it wants. The MAX_HOP it defines for the access technology A is then no useful.

Secondly, each MN in the mobile ad hoc fringe, and each access router of the wireless access network that has wireless interface(s), should keep an Address Mapping Table (AMT). They can glean the MAC-IP mapping information and put into AMT for possible future use. The entries in the table have Hop and Lifetime properties. The AMT is managed by the mobile node or access router according to IP packets passing by. While the MN moves from one place to another place, new entries will be added in, and old non useful entries will be automatically removed when it times out.

Hop	Lifetime	MAC address	IPv6 address	
0				→Its own mapping info
1				→one or more hop mobile nodes' mapping info
...				
MAX_HOP				

For the IP packet, which has "00" indicator in the CLASS field of the IPv6 header, requires normal treatment. This kind of normal IP packet can be used to transfer MAC-IP mapping information with the help of hop-by-hop options header. We don't bring new designed message in the system, so the protocol would be simple and lightweight. Although the transmission of this kind of IP packets will be delayed along the path, but for non real-time sessions, there will be no problem. On the other hand, when the MN gets enough mapping information, or the database has been built up and tends to be stable, there is no need to change the normal IP packets any more.



The MN or access router reads the mapping information from the AMT, and adds one or more entries of the table into the hop-by-hop options header, according to the size of the packet or payload. Simplify, only one entry should be added per IP packet. The entries, which should be informed to other nodes, are those whose "Hop" value is smaller than "MAX_HOP". The entries whose "Hop" value equals with "MAX_HOP", means this mapping information has already arrived at the edge of maximum hop, it doesn't need to be forwarded further.
The header looks like below:

		Opt Type	**Opt Len**
Flags	**Lifetime**		
MAC address (48 bits)			
IPv6 address			

When the MN along the traffic route receives the IP packet, it should check the "Hop" field at first, increases the "Hop" value by 1. The changed mapping information should be added to its own AMT, if this entry doesn't exist; or the entry should be updated, according to the "Lifetime" or new MAC-IP mapping.
If the new "Hop" value equals to "MAX_HOP", then this hop-by-hop options header is no useful, should be removed from the IP packet by the MN, otherwise the header should still be forwarded to the next node on the path.
How does the egress node of the mobile ad hoc fringe get the MAC-IP mapping information of its potential ARs? The principal is the same. The current AR that has wireless interface(s) can provide the information to it. For other routers inside the access network, they have no wireless interface; so they don't recognize this hop-by-hop options header, just simply ignore or remove it from the header.

4. Conclusion

MIAMI is an approach for "Information Dissemination", it is not a "really" address resolution protocol, it just supports to address resolution (MAC <=> IP) in MANETs.

Using MIAMI packets, missing MAC or IPv6 address field in the options header, the MN can actively propagate "Requests" in the ad hoc network. Compared with the "hard" operation of IPv6 ND/IND, it is a "Soft", smooth operation.

MIAMI is "simple, lightweight" designed, it is an automatic, distributed and dynamic mechanism, works as a supplement to IPv6 ND/IND, without much administrative intervention. There is no central server/agent needed. The MNs "proactively" propagate address mapping information, and expand the local cached mapping information, which will minimize the need of IPv6 ND/IND. At the same time, Interaction with local cache, e.g. Neighbor Discovery Cache can actively expand cached information, frequently update, and be suitable to dynamic network environment.

QoS aware handover for IP based ad hoc environments

Yigang Xu
Supervisor: Matthias Riedel (Sony)

March, 2003

Table of Content

Chapter 1. Motivation

Today, the Internet is still the basis of data and communication network. With the fast development of personal communication devices and wireless communication technologies, it is confident and widely accepted that both the Internet and the wireless communication communities are merging towards a single, open and all-IP based wireless mobile Internet architecture, which can support diverse access technologies. Different kinds of smart mobile terminals, like notebooks, mobile phones, PDAs will be connected to the Internet and access the available data and services. The extension of current services into the wireless world is already well underway.

The main drawback of the current Internet is the lack of QoS support. However, QoS support is essential for commercial and real-time applications, such as Internet Telephony and on-line video retrieval. For several years there has been a considerable amount of research within the field of developing the Internet QoS architecture, based on the Integrated Service (IntServ) architecture and the Resource Reservation Protocol (RSVP). However, RSVP and IntServ approaches can't be deployed in large scale Internet backbones due to scaling and billing problems. Another new approach for QoS support in the Internet is Differentiated Service (DiffServ). The problem is that, all these QoS approaches have been designed in the context of fixed network structure, they are not fully adapted to the dynamic mobile wireless environment. The mobile world therefore needs some adaptations.

The former master thesis "Adaptive QoS-supporting Architecture for Real-time Application in Wireless IP Network" proposes a new QoS infrastructure ---Adaptive Reservation and Pre-allocation QoS Architecture (ASAP), it considers QoS support in IPv6 wireless access network.

The goal of this work is to design a QoS-aware handover module for the ASAP QoS architecture, to minimize QoS degradation of adaptive real-time applications due to the mobility of mobile nodes. We extend the considered network architecture to all-IP based future mobile Internet and focus on the mobile nodes roaming in the mobile ad hoc fringe network.

Chapter 2. QoS support in MANET

A mobile ad hoc network is a collection of wireless mobile nodes, which dynamically form a temporary network without the use of any existing network infrastructure or centralized administration. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly changing, random, multi-hop topologies, which are likely composed of relatively bandwidth-constrained wireless links. [RFC2501]

A mobile ad hoc network can be seen as an autonomous system or a multi-hop wireless fringe extension to the Internet. As an autonomous system, it has its own routing protocols and network management mechanisms. As a multi-hop wireless fringe extension, it should provide a flexible and seamless access to the Internet. The goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains.

Mobile ad hoc network has its own advantages, such as high robustness structure and easy way to setup; the disadvantages are obviously resource constraints, like limited wireless bandwidth and power. Recently, since real-time applications, like voice and video are more and more important in mobile network environment, it becomes critical to be able to support these types of traffic also in mobile ad hoc networks. This leads to growing research interest in providing QoS support in MANETs.

The ability of a network to provide specified QoS for real-time applications depends mainly upon the performance properties, such as delay, packet loss, available throughput, error rate of the connection, traffic load within the network, and the control algorithms operating at different layers. A lot of work has been done in the QoS supporting in the Internet, but unfortunately none of them can be directly used in MANETs.

In MANETs, due to the mobility of mobile nodes and the dynamic, keep changing nature of the network topology, real-time packets can be dropped when the network topology is changing rapidly, real-time sessions can be delayed when the traffic routing path is redirected. Furthermore, the quality of a wireless link, e.g., its capacity or signal-to-noise ratio, is apt to be highly variable and the environment conditions influencing wireless links at a particular time are not likely to be known completely or in advance. So it is a huge challenge to provide QoS supporting in MANETs. In one word, the challenge we face is to implement complex QoS functions with limited available resource in a dynamic environment.

Chapter 3. ASAP QoS Architecture

The former work --- "Adaptive QoS-Supporting Architecture for Real-time Applications in Wireless IP Network" develops a new QoS architecture, named as ASAP (Adaptive ReServation And Pre-allocation QoS Architecture). ASAP relates to mobile computing in wireless network environment, where the link quality is unpredictable time varying, ASAP specifies in the field of QoS supporting for adaptive real-time applications running on the mobile nodes. To achieve these, ASAP provides mechanisms of resource pre-allocation, soft/hard reservation, QoS monitoring and adapting QoS related metrics. ASAP can provide sufficient adaptive QoS support to real-time applications in wireless IP access network quickly and efficiently.

3.1 Flow Setup Phase – Soft Reservation

In order to support the QoS requirement of the real-time application, resource reservation or pre-allocation is necessary to be done at first. The real-time application at the source node S informs the bandwidth requirements to the ASAP QoS model, so the model can generate an ASAP Soft Reservation Message (SR). As shown in Figure, for the initial SR message, the MinBW field is 100K, the MaxBW field is 300K, and the Monitored BW field is originally set to 0K. That means there is no reservation done yet on the source node itself. Like RSVP protocol, ASAP QoS model of node S contacts with the traffic control module in the kernel, makes 300K soft reservation for the flow, and then remarks the Monitored BW field in SR message as 300K.

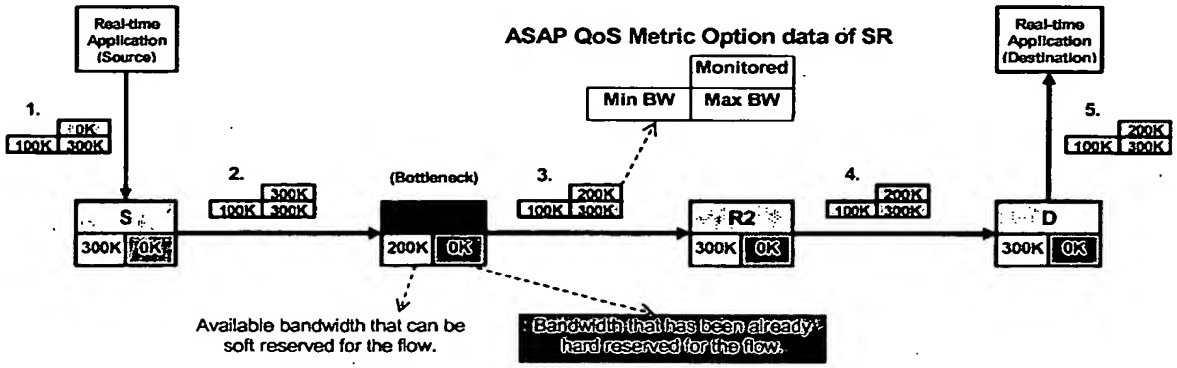


Figure: Signaling of SR for Flow Setup Phase

Depending upon the routing protocol, this SR message will be forwarded toward the destination node D through a selected routing path. Along this routing path, each intermediate network router will process and forward the received SR message to the next hope in the same way.

We assume that intermediate router R1 is the bottleneck which has only 200Kbps available bandwidth. When R1 receives SR message, it finds out that it has only 200Kbps bandwidth available, so it can only make 200Kbps soft reservation for the flow unlike other routers. R1 will replace the Monitored BW field with the smaller value, 200Kbps.

So the number in the Monitored BW field always shows the minimum soft-reserved bandwidth from the source to the current router. If R1 do can provide 300Kbps bandwidth for the flow, it doesn't need to change the Monitored BW field of the SR message, simply makes 300Kbps soft reservation. If R1 can't even afford minimum 100Kbps bandwidth for reservation, it makes no reservation for the flow. It will re-mark the Monitored BW field as zero, and forward the SR message to the next hop.

Finally the SR message arrives at the destination node D, it will do exactly the same thing as the source node and intermediate routers. By checking the Monitored BW field in the SR message, the ASAP QoS model of the node D realizes that the throughput of the traffic path is 200Kbps, and informs the real-time application to make corresponding adaptation.

3.2 Flow Setup Phase – Hard Reservation

After getting the feedback from the real-time application running on the destination node D, the ASAP QoS model of node D can then generate an ASAP Hard Reservation Message (HR) to convert the soft reservation on every intermediate router to hard reservation, so that the flow traffic can use the bandwidth that reserved for itself. In the initial HR message, MinBW field is still 100K, and the MaxBW field is still set to 300K, the meaning of the Monitored BW field is changed from monitor bandwidth to set bandwidth, since the QoS metric option data is now used in HR message. It is set to 200K which is equal to the throughput monitored before.

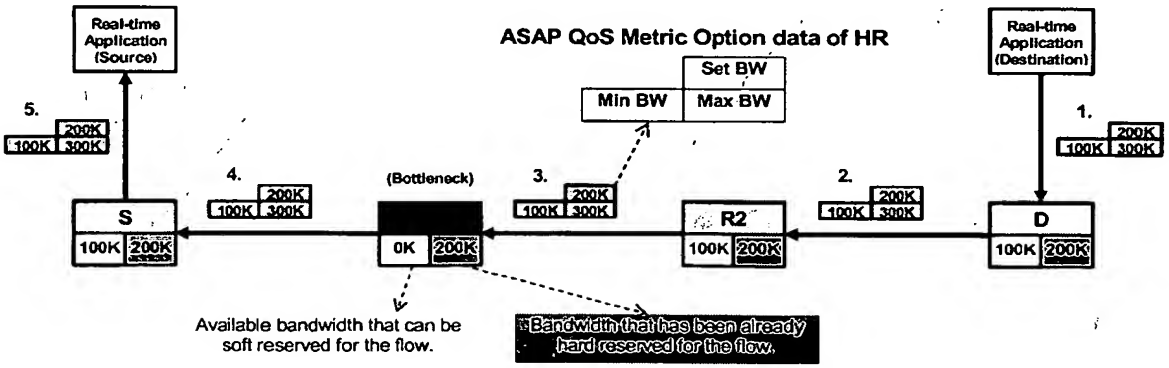


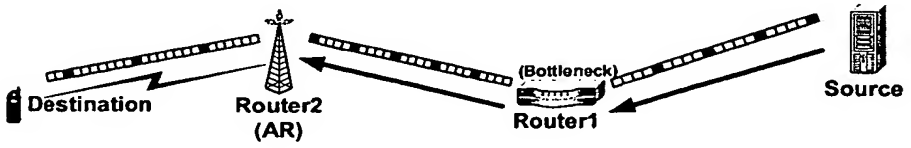
Figure: Signalling of HR for Flow Setup Phase

Upon receiving an HR message, every network router will switch soft reserved 200Kbps bandwidth to hard reservation; the extra soft reservation will be released, like 100Kbps soft reserved bandwidth in D, R2, and S. the HR message will be forward to the next hop along the traffic path. Finally the real-time application running on the source node S will know that 200Kbps is the throughput, it can then adapt to the QoS situation of the path, and send the real-time flow with the corresponding speed and quality.

3.3 QoS Monitoring Phase

After the flow setup phase, resource hard reservation has been done along the traffic path, and the real-time application can now run with a stream level of 200Kbps. But this is not

enough. As discussed before the wireless network is unstable and changes all the time, the real-time application should keep track of the QoS situation of the connection, and could adapt its stream according to the QoS changing, upgrading or downgrading. ASAP QoS monitoring is necessary for the unstable network environment and adaptive real-time application.



□ **Normal Payload Packet**
■ **ASAP QoS Monitoring Packet (SR Messages)**

The SR message can also be used for QoS monitoring. Once the real-time flow is going from the source node S to the destination node D, ASAP QoS model of S will periodically insert SR messages into the flow. Every SR message is used to collect the QoS information along the traffic path, when arriving at destination node D, SR message informs the real-time application about the current throughput at each time period.

We still use the example in flow setup phase to briefly describe QoS monitoring phase. The bottleneck of the traffic path is router R1, in the later time the QoS situation on R1 maybe better, it gains 100Kbps available bandwidth or more; or maybe even worse, it loses part of existing bandwidth and can only provide 150Kbps bandwidth or less to the flow. All these changes can be reflected in the Monitored BW field of SR message, captured by the ASAP QoS model and informed to the real-time application running on the node D. The real-time application could upgrade or downgrade its stream to the corresponding level immediately according to its adaptation strategy, and ASAP QoS model can generate and forward HR message to the source node S, and let the intermediate routers along the traffic path make corresponding new hard reservation for the flow.

Chapter 4. Design Requirements and Assumptions

4.1 Design Requirements

The QoS-aware handover module includes the issues in the following aspects: geographically adjacent access router (GAAR) discovery, candidate access router (CAR) discovery, target access router (TAR) discovery, context transfer (CT), resource pre-allocation (Soft Reservation), reservation confirmation (Hard Reservation) and of course reservation release. The layer 3 QoS-aware handover module should fulfill the following requirements:

"Independent"

(1) It MUST be an interoperable solution that works for any Layer 2 radio access technology, because mobile nodes MAY have wireless interfaces belonging to different technologies, e.g. Bluetooth, HiperLan/2.
(2) It MUST be able to use either Layer 2 or Layer 3 events to trigger or initiate the handover procedures. The trigger mechanism MUST hide the specifics of any L2 trigger mechanisms, not utilize any specific L2 information.
(3) It MUST not depend on a particular mobility management protocol, not depend on a feature, which is unique to a particular mobility management protocol.

"Anticipated"

The advantage of "anticipated" is that the handover can be executed quickly, because much of the information is collected in advance of handover procedures. Context information about the mobile node's packet session MUST be transferred from the old path to the new path, to quickly re-establish services, rather than require the mobile node to establish services along the new routing path from scratch. This could minimize the impact of the traffic redirection, and minimize the service disruption due to the handover procedures.

"Adaptive"

It MUST be able to adaptive to the changes in network topology and resource availability, so that it can react to QoS violations, which MAY occur frequently in wireless environments due to changed environmental and network conditions.

"Flexible"

It SHOULD provide mobile node's requirements or preference, e.g., least cost policy. It SHOULD consider the need of adaptive real-time applications or access routers, e.g., load balancing, resource intensive applications.

"Scalable"

It SHOULD be able to cope with the fast growth of the network. Not only working in the mobile ad hoc fringe network, even for a large-scale network with thousands of mobile nodes, the functionalities and performance of the QoS-aware handover module SHOULD not be greatly reduced.

"Simple and Efficiency"

"Intelligent terminal and dumb network". Keeping the network intact as much as possible and pushing the changes to the end nodes is practical, this is the normal way for a new designed protocol to be easily deployed into an existing world with other protocols running. At the same time, as fewer possible network entities involved, the module requires fewer protocol exchanges, minimizes the amount of signaling and processing load. The reliability, resource utilization and completion delay COULD also be improved. It SHOULD also be lightweight in resource requirements of mobile nodes and easy to implement.

"Robust and Secure"

It SHOULD be a handover solution that satisfies:

(1) Secure network entities' capability transfer. Security provisioning includes protecting the integrity, confidentiality, and authenticity of the transfer.
(2) Secure QoS requirements' expression.
(3) Conform and inter-operability with existing IETF security policies and protocols.
(4) No single point of failure, the system SHOULD be able to cope with different predictable or unpredictable errors. There SHOULD be quick automatic recovery from network node and link failures.

4.2 Assumptions

If the topology of an ad hoc network changes too fast, the provision of QoS is even impossible. However, QoS is feasible in many cases where the network topology changes less frequently. In this paper, we assume only study the type of ad hoc networks whose topologies are relatively stable, not changing too fast to make the QoS supporting meaningless.

Two mobile nodes are neighbors and have a wireless link between them if they are in the transmission range of each other. Each mobile node periodically transmits a BEACON signal to identifying itself. We assume by the help of IPv6 Neighbor Discovery Protocol (ND) and Inverse Neighbor Discovery Protocol (IND), any mobile node can know the set of its neighbors. Neighboring nodes share the same wireless access technology and media. We also assume the existing of a lower layer protocol, which resolves the media contention, supports resource reservation.

In the mobile ad hoc network, the bandwidth problem is a very important issue. Due to mobility and radio properties, the bandwidth information is changed dynamically, thus to maintain the QoS of a connection is more difficult than in a cellular network. Bandwidth guarantee is one of the most critical requirements for real-time applications. The bandwidth calculation and reservation are the first step for further control in such an environment. So in this paper, we only consider "bandwidth" as the QoS parameter, omit Signal to Interference Ratio (SIR), packet loss rate, etc. The goal of the QoS-aware handover module is to find the best routing path among all potential paths on which the available bandwidth is the maximum, supporting the QoS requirements of real-time applications.

Chapter 5. QoS-aware Handover Module

The QoS-aware handover module is designed for ASAP QoS architecture (Adaptive Reservation and Pre-allocation), which relates to the field of supporting QoS for adaptive real-time applications running on mobile nodes in dynamic, mobile wireless IP networks where the quality of the node connectivity is unpredictable time varying.

Due to the mobility of the mobile nodes, handover inevitably happens. In ASAP, before communication session is established, the resource reservation should be done on the flow path in advance. When handover occurs, the access point of the mobile node changes, then the flow path needs to be redirected also. On the new flow path, unfortunately there could be no corresponding resource reservation done for the flow, and this will lead to significant QoS degradation for the real-time application. So, the main task of QoS-aware handover module of ASAP QoS architecture is how to make resource pre-allocation along the new routing path of the flow.

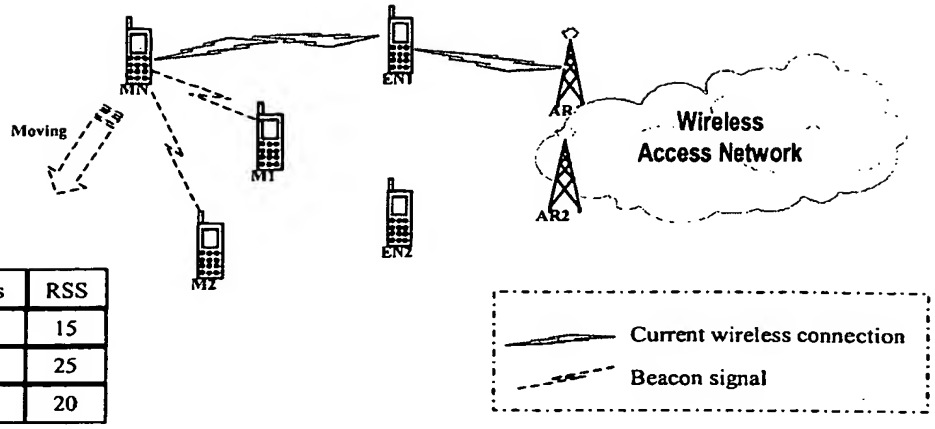
5.1 QoS-aware Handover Procedures

The QoS-aware handover module includes below several procedures, they are:

- Neighbors detection, handover candidate nodes selection
- Handover initiation
- QoS metrics probing along each potential routing path, resource pre-allocation (soft reservation) on the potential paths
- QoS metrics collection
- Handover decision, handover target node selection
- Reservation confirmation (hard reservation)
- Reservation release

5.1.1 Neighbors Detection

The QoS-aware handover module is independent upon layer 2 access technologies. The handover procedures can be triggered by layer 2 events or layer 3 events, the module is independent upon any kinds of handover triggers. . Here in the figure below, we give an example on how layer 2 trigger comes to initiate the handover.



MAC Address	RSS
EN1	15
M1	25
M2	20

Figure: Candidate Nodes Finding

The quality of wirel tor, called Received Signal Strength (RSS). Besides of MAC address, RSS is another useful parameter that assumed can be retrieved from the received BEACON signals by the mobile node. When the MN connects with the current mobile node EN1 for communication with CN, it still keeps on monitoring the RSSs of the surrounding neighbors, including the current connection. With these BEACON signals, the MN can know the existence of its neighbors, and keep an active candidate cache, a list of all of potential handover candidate nodes and their RSSs. Once the RSS of a neighbor is stronger than the add threshold, the node can be added in the cache. When the RSS is below the remove threshold for a time period, the node should be removed form the cache.

Assuming the current wireless link turns to be in a bad situation, the RSS of the current connected node is below the remove threshold for a while and the node EN1 needs to be removed from the candidate list, and then this layer 2 event will be captured by the QoS-aware handover module, used to trigger the handover procedures immediately. Together with the handover trigger, the list of all the potential candidates that have "stable" strong RSSs over the threshold is also passed to the QoS-aware handover module. The capability of these candidates will be probed in the later stage and the final handover target node will be selected from this list.

5.1.2 Handover Initiation Procedure

In the normal case, the candidate who has the highest RSS will be used as the handover target node. Layer 2 handover will then occur, the MN will disconnect with the current node and connect to this selected target node, and network layer handover occurs after the L2 handover finished. The target node will take over the role of forwarding the flow packets generated by the MN. After that, the handover procedures are over.

But for real-time applications, things should not be treated so simply. RSS should not be the only factor to consider, which means the node with the highest RSS maybe not the handover target node. In QoS-aware handover, not only the RSSs of the candidates, but also the QoS capabilities along the routing paths towards the candidates should be checked and investigated. The one who has the strongest RSS but very bad QoS capability is not the right handover target. From the point of view of real-time

applications, the QoS capability of the handover candidate is a more important parameter than the RSS. The QoS metrics probing is the most important procedure for the QoS-aware handover module.

For mobile ad hoc networking, there are frequent changes of network topology due to the mobility of mobile nodes. We also know, the wireless air link condition is always unstable and narrow bandwidth. Besides these, the mobile node has internal problems of battery power limitation and weak processing capability. Further more, another main consideration is the limitation of simultaneously connectivity of the mobile node. If we simply use the mobile node to probe the QoS metrics of each candidate, that means, the mobile node could have to carry out unwanted L2 handover procedures several times to enable to send the probing packets to the candidates. The caused latency and processing load may be huge to the mobile node. So, in such a complicate mobile wireless environment, it is not a wise choice to let the mobile node probe the QoS metrics and bear huge processing load. These are the reasons why we prefer to let the correspondent node (CN), but not the mobile node (MN) to enable the QoS metrics probing.

The reason why we use end-to-end handover negotiation, but not inform one intermediate node, for example EN1 to probing the QoS metrics of each candidate is a little simple. First, the intermediate node could also be a mobile node in the ad hoc fringe. Second, the probing result from the intermediate node to the candidate node does not exactly show the QoS situation of the potential routing path. The intermediate node probes not on the right routing path from the CN to the MN. Later to enhance the QoS-aware handover module, we could try to find a crossover ASAP-enable router with the help of mobility management to limit the handover negotiation and process overhead. This could be very useful.

Shown in the figure below, the role of MN after receiving the handover trigger is just to send the handover initiation signal to the CN, passing the candidate list and the target node for resource reservation to the CN. Of course in the message the flow ID or desired QoS metrics can also be passed to notice the CN.

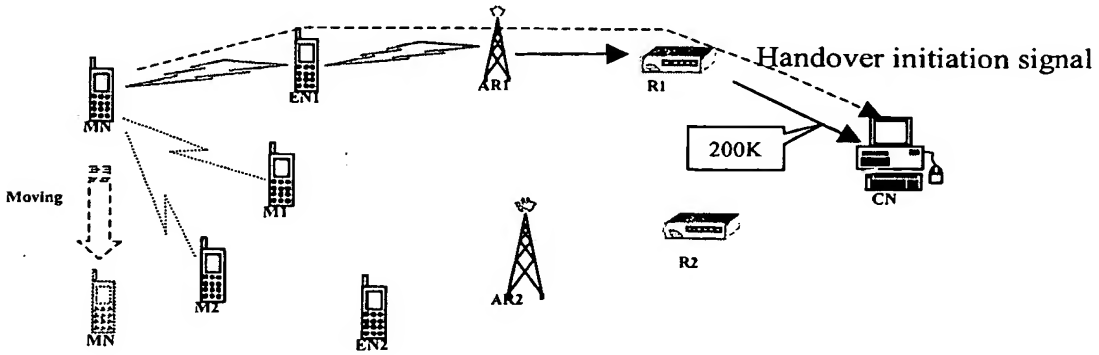


Figure: Handover Initiation Procedure

5.1.3 Handover QoS Metrics Probing Procedure

In the last section, we have already discussed why it is better and necessary to use the CN to probe the QoS metrics of each handover candidate. After receiving the handover initiation signal sent from the MN, the CN can begin the probing procedure. See the below figure.

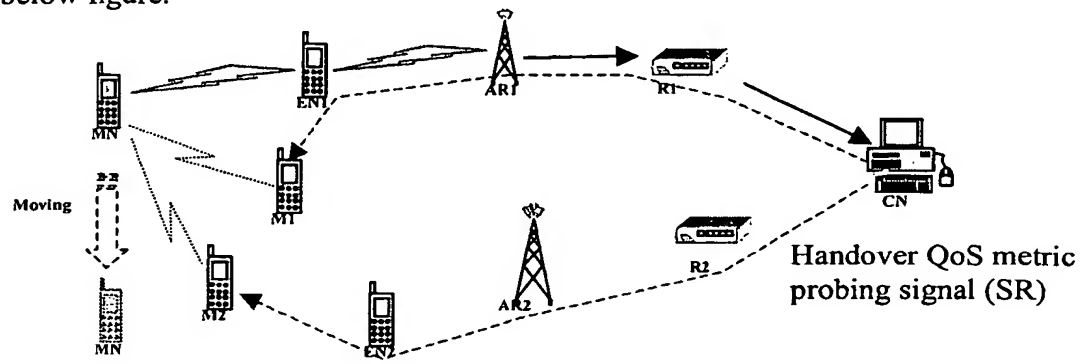


Figure: Handover QoS Metrics Probing Procedure

According to the routing protocols of the Internet, wireless access network and mobile ad hoc network, the CN can find a routing path toward each candidate and probe the new path. The new routing path could be a path using part of old routing path or a "brand-new" path. What is important is that the probing signal along each potential routing path should find out how much QoS metrics is available and can be soft reserved for the flow, and save the path history with the help of the address option data in the packet header.

Unlike the handover initiation signal using IPv6 destination options header, the handover QoS metrics probing signal uses IPv6 hop-by-hop options header, this is similar to QoS monitoring procedure in ASAP. The probing message contains the flow ID information. Upon receiving such a probing message, the intermediate node checks the Flow ID in the message and its local cached QoS table. If a QoS entry with the same Flow ID already exists, that means this intermediate node is on the current routing path, e.g. R1, AR1, EN1. The node should not simply bypass the probing message without processing, it should check current QoS situation and find if there exists QoS upgrading or downgrading. If the Flow ID is new to the local QoS table, this node must be on the new path, e.g. R2, AR2, EN2, then the intermediate node should make the corresponding soft reservation for the flow ID according to the QoS requirements of the flow. The IPv6 address in the address option data of the header indicates from which one-hop neighbor node this probing message is sent, this address information should be saved also in the QoS table to keep the path history. Before the intermediate node forwarding the message out to the next hop, it should replace the address option data with its own IPv6 address.

When the candidate node receives the probing message, it works in the same way as the intermediate node, saving the path history, making the corresponding soft reservation for the flow ID toward the target, which is also indicated in the address option data of the header. So far, the candidate node has the complete knowledge about how much QoS

metrics is available and soft reserved on the new potential routing path from the CN through itself to the MN.

One point to mention, how does the node, intermediate node or candidate node, make soft/hard resource reservation for the flow? It is out of the scope of ASAP QoS architecture. Like RSVP protocol, the ASAP QoS architecture has the interface with the "traffic control module" of the kernel. The kernel could be Windows, Linux or Cisco router. The traffic control module takes charge of "real" task of resource reservation. Dependent upon what kinds of resources to be reserved, the traffic control module may use L1-L3 technologies. This is a device- and technology- dependent issue and is not dealt with by ASAP.

5.1.4 Handover QoS Metrics Collection Procedure

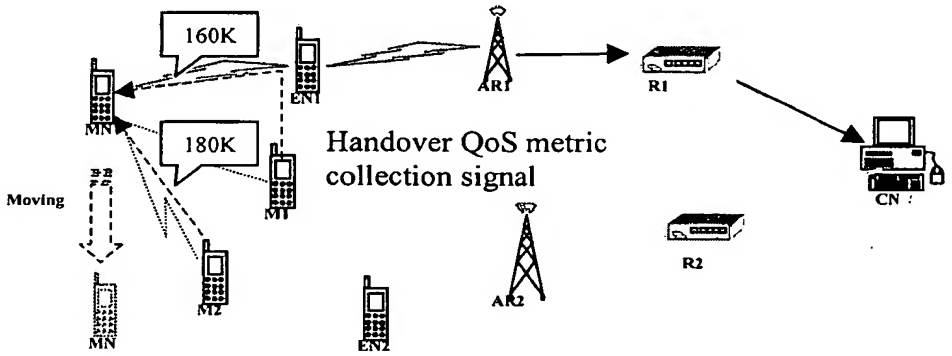


Figure: Handover QoS Metrics Collection Procedure

Once each candidate, e.g. M1, M2, finishes processing the QoS metrics probing message, it will immediately reply with another message to the target (MN), this message is called QoS metrics collection signal. It is similar to the handover initiation signal, using IPv6 destination options header, used to inform the MN its QoS capability. The amount of soft reserved resource of the path is marked in the Monitored QoS metrics field of the message header. The QoS metrics collection signal could be sent to the MN through any exist wireless link, no matter direct connection or forwarding by other mobile nodes.

5.1.5 Handover Decision Procedure

When the MN receives each QoS metric collection signal from each candidate, e.g. M1 and M2 in the example, the MN will know that 160Kbps bandwidth is available on the path from the CN to itself through M1, and 180Kbps on the path through M2.

The MN can then make the handover decision to select the candidate node, which has the highest available QoS metrics on the routing path, as the handover target node. In this example, 180Kbps bandwidth is available on the path through M2, which is more than 160Kbps through M1. So, M2 is selected as the target node.

If the result is different from the throughput of the current routing path, in the example, the current throughput is 200Kbps, but after the handover, when the MN changes to connect with M2, the throughput will be changed to 180Kbps, then the result should be submitted to the real-time application not only running on the MN itself, but also running on the CN. So the real-time application could be informed about the incoming handover and the throughput on the future new routing path, and the real-time application can prepare to adapt to the changes.

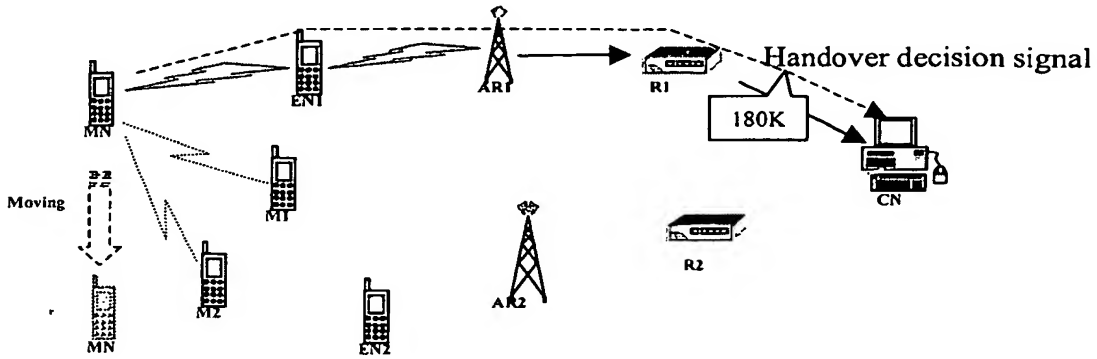


Figure: Handover Decision Procedure

In the figure above, the MN sends a handover decision signal to inform the other end of the real-time application. This message is also similar to the handover initiation signal, using IPv6 destination options header, tells the CN that the real-time application should prepare to the incoming throughput 180Kbps. And the application will send an 180Kbps stream instead of original 200Kbps. Otherwise, excessive flow traffic will overload the path and cause flow interruption and packet loss.

If we assume that, the new routing path from the CN to the MN through M2 can also provide 200Kpbs bandwidth as the current path, then the MN doesn't need to inform the real-time application on the CN, the handover procedure is transparent to the higher layer, the real-time application ignores whether or not the handover happens, it just send the flow traffic at 200Kbps as before.

5.1.6 Handover Confirmation Procedure

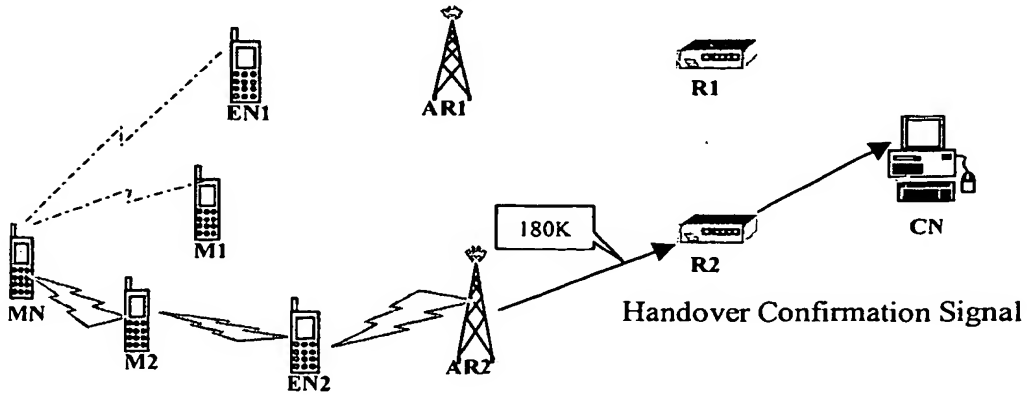


Figure: Handover Confirmation Procedure

Then the MN can drop its current wireless connection with EN1, and build the new connection with M2. A handover confirmation signal with a bandwidth request 180Kbps will be sent with the flow traffic from the MN to the CN through M2. This handover confirmation signal adopts IPv6 hop-by-hop options header, similar to the handover QoS metrics probing signal, which is used as soft reservation message (SR). With this handover confirmation message, the soft reservation on the new path from the MN, through M2 to the CN will be switched to hard reservation. This signal is used as hard reservation message (HR).

When the CN receives the handover confirmation message, the QoS-aware handover can be considered to complete.

5.1.7 Reservation Release Procedure

Actually the whole handover procedure is not yet finish. The last step to be considered is how to release the reserved resource. In our example, the resource from the MN through EN1, AR1, R1 to the CN is hard reserved for the flow, and the resource from EN1, M1 to the MN is soft reserved. These two reservations should be released quickly after the handover, so that the released resource could be used by other traffic flows.

The resource reservation managed in ASAP is "soft state", so there are two ways to release the reservation. One solution is to send an explicit message for the releasing. We can use a special hard reservation message (HR). In this HR message, the bandwidth request is set to zero. The MN sends this HR message along the old path to the CN, and the occupied resource along the old path can be released. Of course these should be some necessary mechanism, such as sequence number to make sure that the old reserved resource is correctly released, but not the new reserved for the same flow. This solution is suitable to release the hard reserved resource in mobile ad hoc network environment, which has the limitation of resource. When the real-time application accomplishes, we can also use this solution to release all the reserved resource of the flow.

The other solution is quite simple and no extra signaling is needed, it just let the reservation times out, as it is soft state. But obviously this is not a really efficient way to do releasing, because when the mobile node tends to have severe resource competitions, the immediate resource release becomes quite necessary. On the other hand, this solution is only suitable to the soft reserved resource, but not the hard reserved resource.

5.2 QoS-aware Handover Signaling Format

5.2.1 ASAP Messages [ASAP]

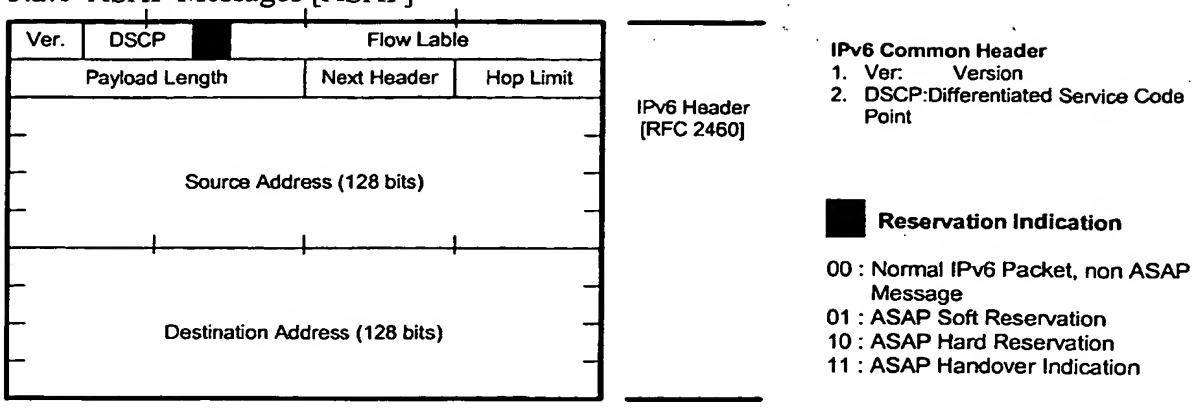


Figure: RI Field in IPv6 Header

According to [RFC2474], the first 6 bits of the CLASS field in IPv6 common header are defined as the DSCP (Differentiated Service Code Point), and last two bits are unused. ASAP uses these two bits as a reservation indicator (RI), illustrated in Figure above. There are four codes defined in the RI field:

00: Normal IPv6 packet, Non ASAP Message
01: ASAP Soft Reservation Message (SR)
10: ASAP Hard Reservation Message (HR)
11: ASAP Handover Indication Message (HI)

5.2.2 Two Options Data Defined in ASAP

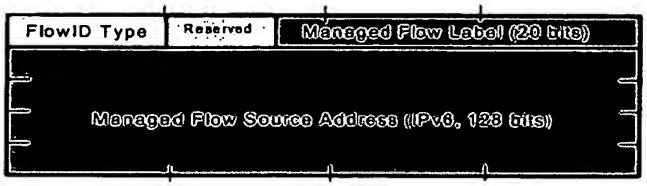


Figure: ASAP Flow ID Option Data Structure

Figure: ASAP QoS Metrics Option Data Structure

5.2.3 ASAP Address Option Data

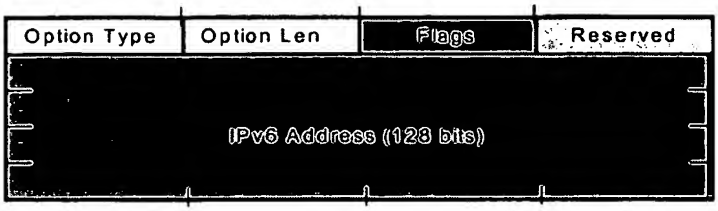


Figure: ASAP Address Option Data Structure

One new option data is defined for the QoS-aware handover module, it is ASAP address option data, shown in the above figure. This address option data carries IPv6 address information, to submit address information, which is useful in the QoS-aware handover procedures.

Flags of the option data indicate three address types or three usages of the included IPv6 address. They are:

(1) Target node address (T), used in handover initiation procedure and handover QoS metrics probing procedure to indicate the candidate nodes to which node they should soft reserve the requested QoS.

(2) Candidate node address (C), submitted by the MN to inform the CN to which nodes it should send out probing messages.

(3) Sending node address (S), used in handover QoS metrics probing procedure. This field is changed hop-by-hop to save the path history of the potential routing path.

5.2.4 QoS-aware Handover Signaling Format

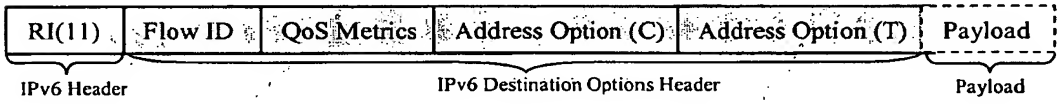
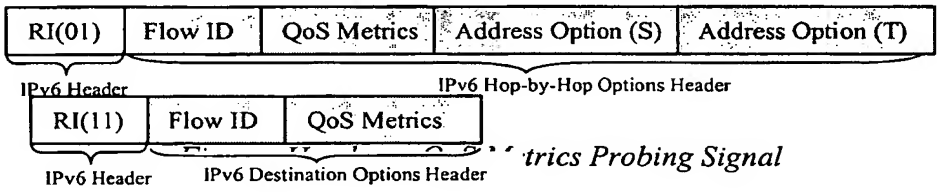


Figure: Handover Initiation Signal



trics Probing Signal

Figure: Handover QoS Metrics Collection Signal
Handover Decision Signal

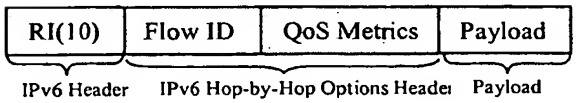


Figure: Handover Confirmation Signal

The above figures illustrate all signals used in QoS-aware handover module, we give the name to the signal according to its functionality, the detail is described in the section 2: QoS-aware Handover Procedures.

5.3 Signaling of QoS-aware Handover

The signaling for the whole QoS-aware handover procedures is shown in below figure.

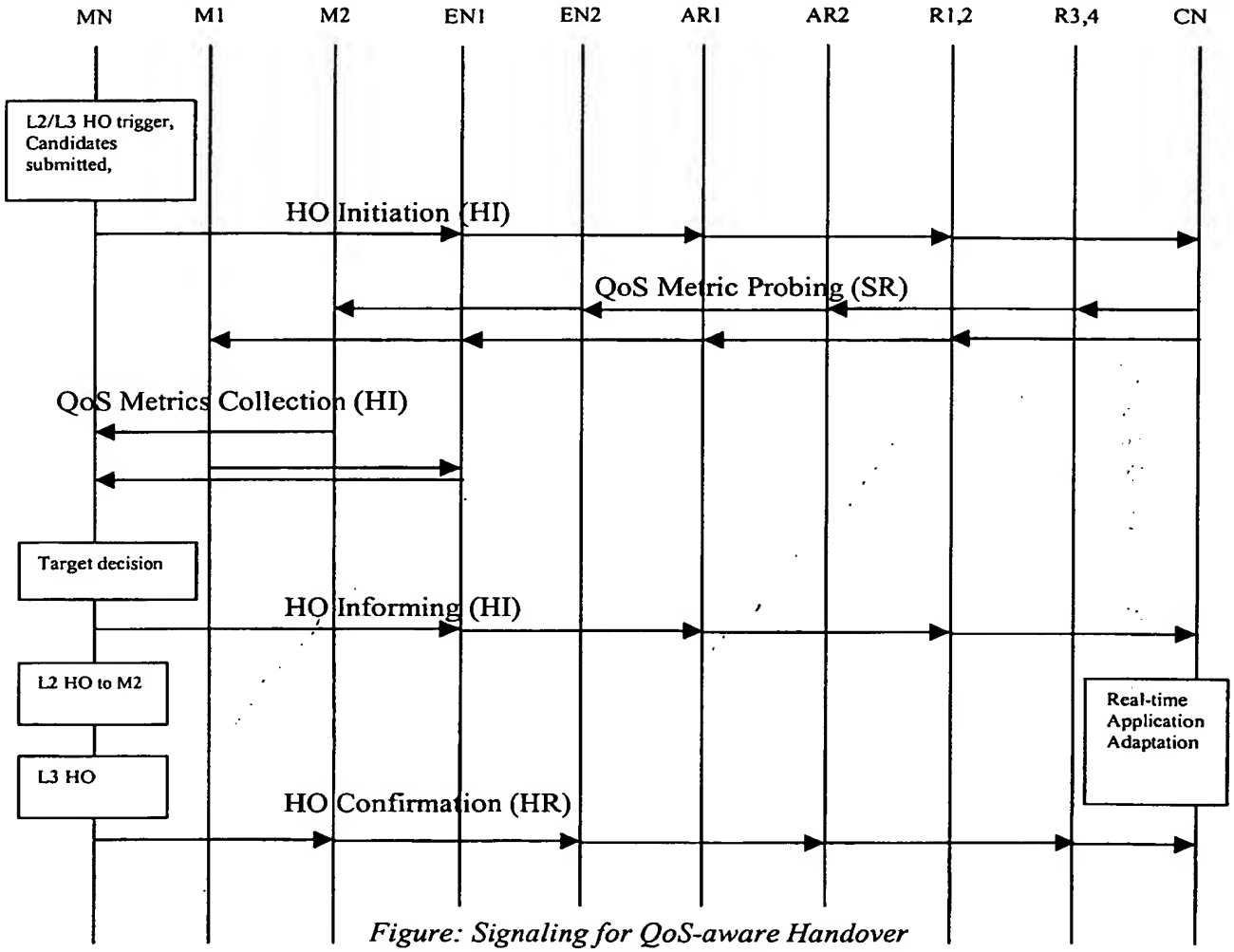


Figure: Signaling for QoS-aware Handover

The handover procedure could be divided into three phases: handover measurement phase, handover decision phase and handover execution phase. Handover measurement and decision phases are more layer 2 related, they are out of the scope of this master thesis, as we said, we focus only on the layer 3 handover execution phase.

After receiving the handover trigger, QoS metrics probing is performed first before layer 2 handover process happens. QoS information on each potential routing path is collected at the MN. With the aid of this information, the target handover node that can provide the

best QoS support will be selected. Then in the following steps, the MN will break the current connection and build the new wireless connection with the target node. After that layer 2 and layer 3 handover processes can begin immediately, the real-time traffic flow will be transferred on the new path.

The timetable of the QoS-aware handover module is shown in the below figure.

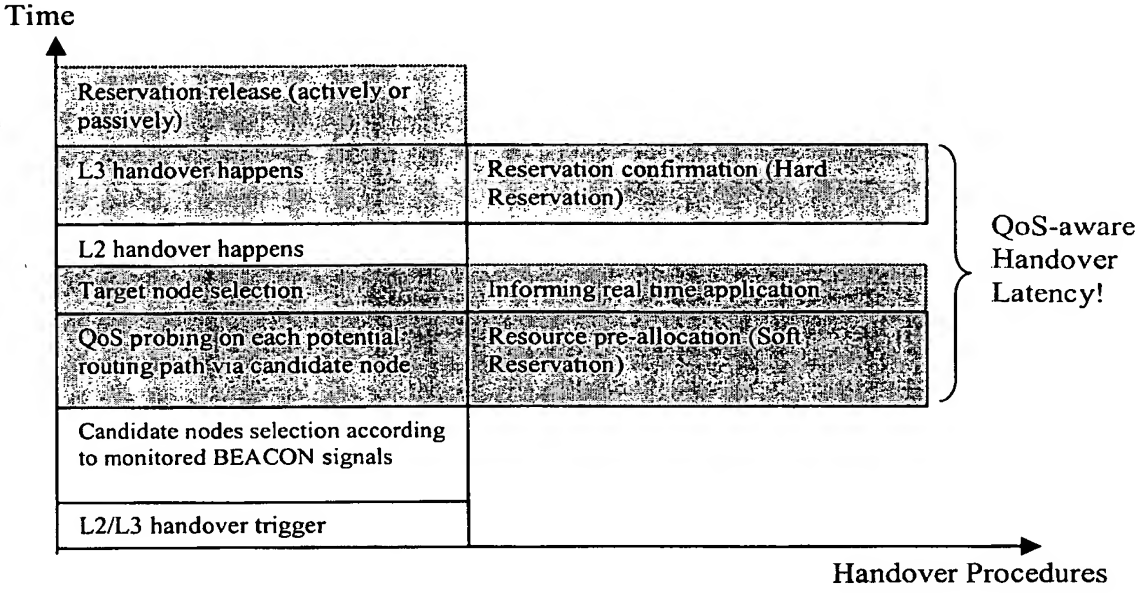


Figure: Timetable of QoS-aware Handover Procedures

Compared with the normal handover process without QoS consideration, which just simply picks up the one with the strongest RSS as the handover target node, the handover latency caused by QoS-aware handover module is spent on QoS metrics probing procedure, which helps to find the best handover target node. During the QoS-aware handover latency, layer 2 handover does not happen, the MN does not break the current connection, so there is no packets loss. Layer 3 handover will happen as soon as layer 2 handover finished. So, the real-time application will not be injured.

5.4 "Local Recovery"

In the above example of QoS-aware handover module, we only focus on the case that the MN is the source or sink node of the flow. But in the mobile ad hoc network, all nodes are mobile, so we should pay attention to the case that the intermediate node is moving away, which also causes the flow path to be redirected.

To resolve this problem, we propose "local recovery", which shares the same principle with the above mentioned QoS-aware handover module. So, we simply point out the difference using the below figure.

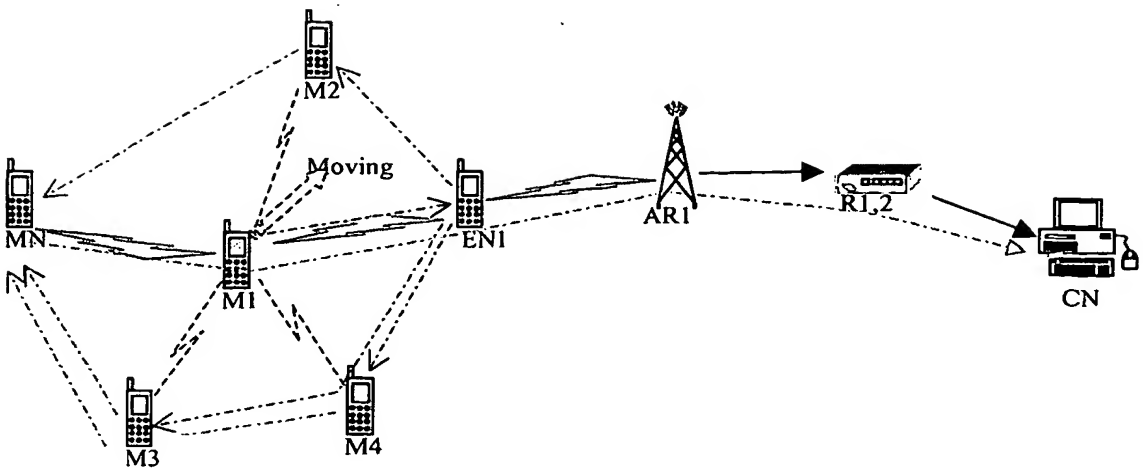


Figure: Signaling of "Local Recovery"

In this example, the current flow is setup between the MN and the CN. Now the intermediate node M1 decides to move away. When M1 gets the L2 or L3 handover trigger, it sends out the handover initiation signal to the one-hop neighbor, e.g., EN1 on the path, not to the CN. In the handover initiation signal, M1 should inform EN1 the required QoS metrics, its candidate nodes and the target node, here the target node is not the moving node M1 itself, but the other one-hop neighbor on the flow path. When receiving the initiation message, EN1 will then probe the QoS metrics on the path towards each candidate node, such as M2, M3, M4. According to the target address in the address option data of the handover QoS metrics probing message, the candidate node can reserve the resource towards the MN. After the reservation, the candidates should inform the MN the probed results in the handover QoS metrics collection signals. With these results, the MN can make the handover decision, and select M3 as the handover target node. The handover decision signal is used to inform M1 that it can move away, and also used to inform the real-time application running on the CN to adapt to the changed QoS metrics if necessary. Then the MN can break the connection with M1, execute L2 and L3 handover to the new node M3. The handover confirmation signal is sent along the new path to change the soft reserved resource to hard state.

Using "local recovery", we can resolve the path redirection due to the mobility of the intermediate node, the handover negotiation is limited in the one-hop range of the moving node, so the handover latency and process overhead can be greatly minimized. Compared with "local recovery", the QoS-aware handover of end node can be also used in the flow setup procedure of ASAP.

The signaling of "local recovery" is illustrated in the below figure.

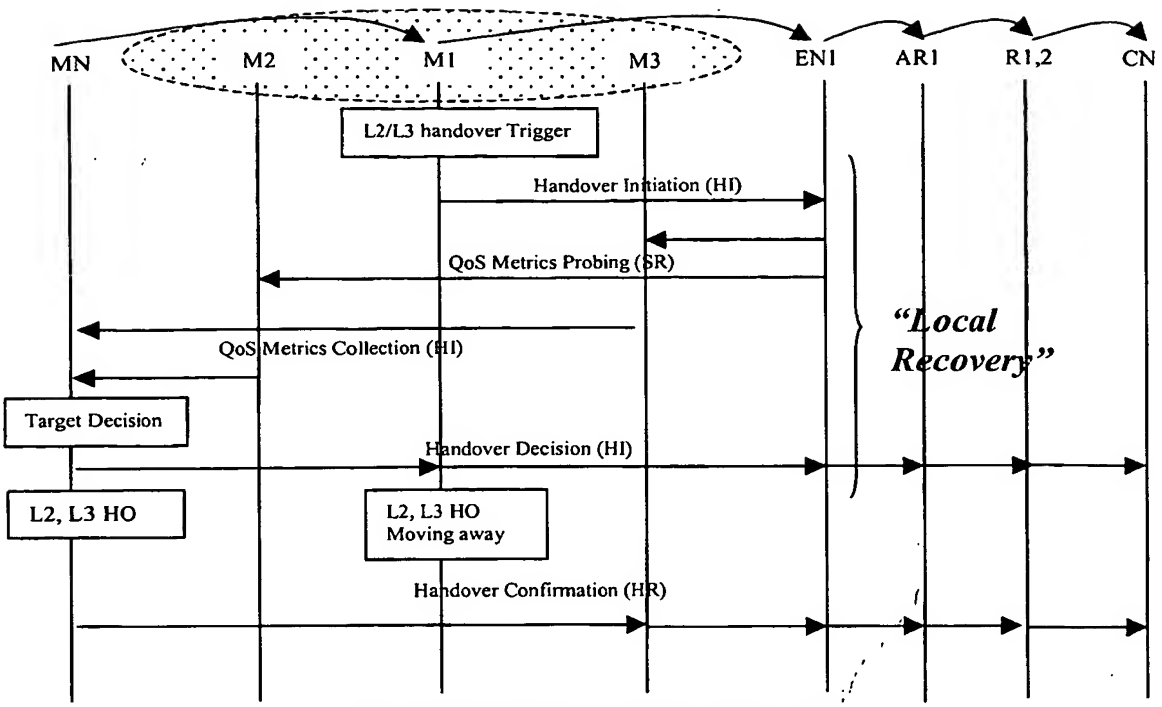


Figure: Signaling of "Local Recovery"

5.5 Comparison

5.5.1 RSVP Standard in Mobile Environment

RSVP is a "Receiver-Oriented" protocol. For RSVP in mobile, wireless network environment, when the receiver (MN) performs a handover that incurs a path change, the new path to the MN from the sender (CN) is discovered by RSVP only after the soft state timers expire in network elements such as routers. This mechanism is so slow that it may cause large delays with frequent host mobility in the network. The problem can be avoided by the mechanism that the CN triggers the transmission of a PATH message after receiving a binding update message from the MN at its new location. The MN can then send a RSVP message back along the new path to the CN for resource reservation.

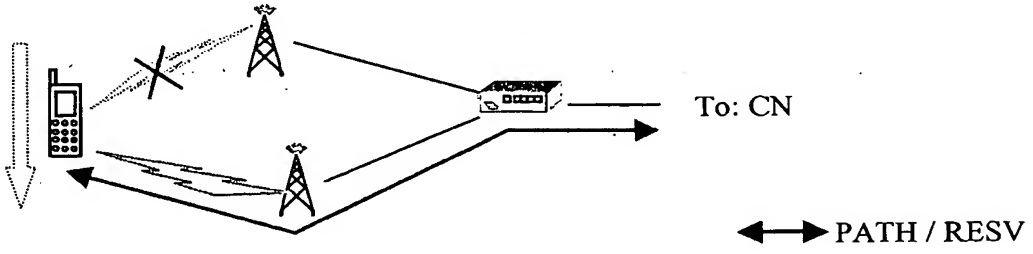


Figure: RSVP Standard in Mobile Environment

"Local repair" of RSVP provides fast adaptation to routing changes without the overhead of shorter refresh periods e.g., reducing the soft state timer. "Local repair" let the local routing protocol module notify RSVP of route changes for particular destinations, and RSVP use this information to trigger PATH/RESV refreshes for these destinations, using the new route. So, "local repair" works in "Break-Before-Make" mode, the great number of packets loss is inevitable, and the resource reservation delay is still long.

5.5.2 RSVP Extensions

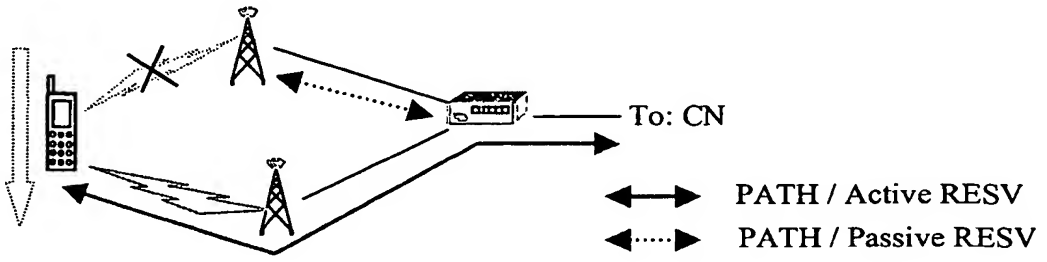


Figure: RSVP Extension in Micro-Mobility

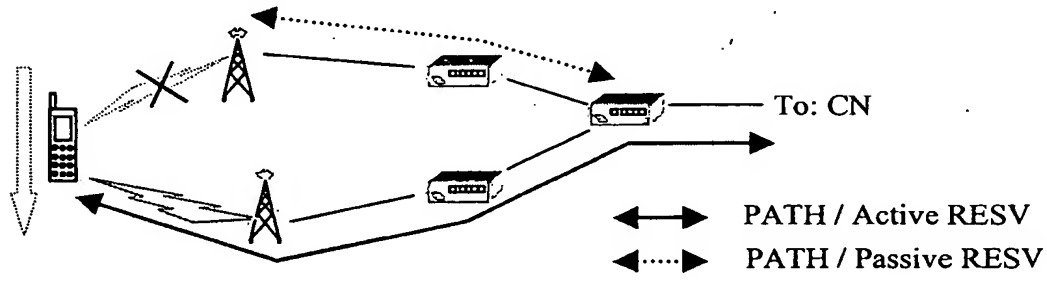


Figure: RSVP Extension in Macro-Mobility

Several RSVP extensions are proposed to modify and enhance the RSVP protocol under the micro-mobility or macro-mobility. Two kinds of reservation are used: passive and active reservation.

Under micro-mobility, active reservations is made between the BS and the MN, the BS is in charge of making passive reservations with all the BSs in the neighboring cells. Once the MN moves in a neighbor cell, both the MN and current BS know that a handoff occurred. At this point, PATH and RESV messages are used to exchange the reservation state.

Under macro-mobility, it is necessary for the RSVP extension, like Mobile RSVP (MRSVP) to specify the set of locations, where the MN may visit in future. The MN needs to establish paths with sufficient resources to these locations. When the MN arrives at new place, the path to that attachment becomes active and the path to the previous one

becomes passive, so the data can still be delivered effectively. But this approach has the problem that many resources are reserved but may never be used even though they are available for other requests.

"Advance Resource Reservation" concept is used in the RSVP extensions. Like RSVP standard under the mobile environment, these approaches are still in "Break-Before-Make" mode between BS and the MN, the data packets can be lost. Furthermore, for making advance resource reservation, an efficient partial path discovery mechanism is required, otherwise the approaches will cause inefficient resource reservation in advance and huge overload for BSs to maintain Active/Passive reservation state information during handovers.

5.5.3 INSIGNIA

INSIGNIA is an IP-based QoS framework that supports adaptive services in mobile ad hoc networks. The framework is based on an "in-band" signaling and "soft-state" resource management approach that is well suited to supporting mobility and end-to-end QoS in highly dynamic environments where the network topology, node connectivity, and end-to-end QoS are time varying. [INSIGNIA]

As shown in the below figure, if a MN in the mobile ad hoc network moves out of radio range of the currently connected mobile nodes, the forward node will interact with the routing protocol and forward flow packets along a new route to the receiver.

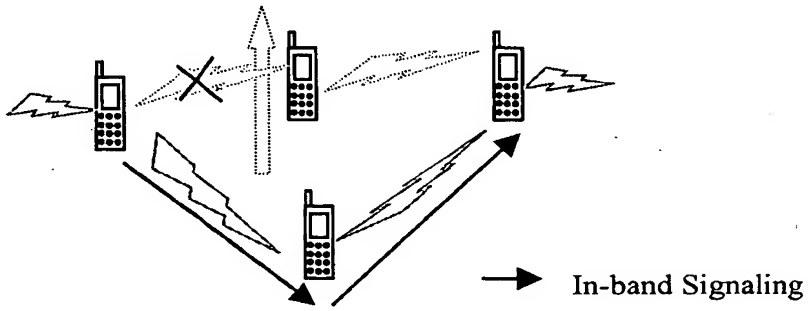


Figure: Rerouting in INSIGNIA

As we can see, the rerouting and restoration algorithm in INSIGNIA is based on the routing protocol to find next-hop, and coupled to the speed at which the routing protocol can discover a new path. It works also in "Break-before-Make" mode, and if the flow is rerouted to a mobile node where resource is unavailable, the flow will be degraded to best effort service, so there is no guarantee to the running applications.

5.5.4 QoS-aware Handover with "Local Recovery"

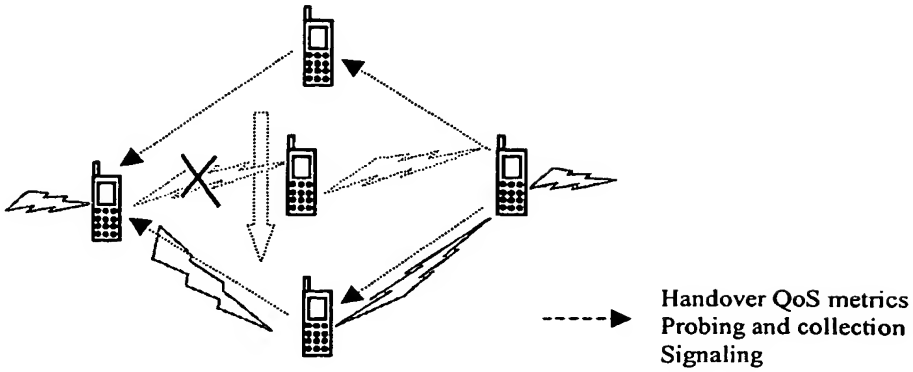


Figure: "Local Recovery" in QoS-aware Handover Module

The QoS-aware handover module is independent of any mobility management. It is neither sender-oriented nor receiver-oriented protocol. The mobile node on which a handover performs could be end node of the flow, or intermediate node with the flow hosting on it.

QoS-aware handover of end node uses end-to-end handover negotiation; the resource is reserved on the routing path between the MN and the CN, which is optimized by the routing protocol. Of course, the round-trip signaling may cause long resource reserved delay, the problem can be minimizes by finding a crossover ASAP-enable node, limiting the handover negotiation between this node and the MN. "Local Recovery" is proposed to deal with the intermediate node mobility, which further localizes and limits the handover negotiation within a small range of the moving node, provides fast adaptation to the changing mobile ad hoc network environment.

Like INSIGNIA, QoS-aware handover module is based on "soft state" for efficient resource reservation management. It combines "in-band" and "out-band" signaling approaches, according to the role of the node and the flow traffic direction, in-band or out-band signaling can be flexible adopted for passing handover control information and resource reservation management information. The most important is the QoS-aware handover module is a "Make-Before-Break" handover model, resource is pre-allocated along the potential path, so no packets loss happens, no injure to the adaptive real-time application.

5.6 Conclusion

QoS-aware handover module is designed as a Layer 3 handover protocol, which is independent of any L2 wireless access technologies, independent of any particular mobility management. It focuses on the QoS supporting for the adaptive real-time applications in the mobile ad hoc fringe network.

The QoS-aware handover module is a seamless handover model. The handover information is "anticipated" collected in advance of L2/L3 handover, e.g., the candidates' IPv6 addresses along with their capabilities are provided to the handover decision node for the handover target node selection. At the same time, resource is "pre-allocated" along each potential routing path. Using the concept of "Local Recovery", it adapts to changes in network topology and resource availability, reactive to QoS violations.

Similar to INSIGNIA, the QoS-aware handover module uses "in-band" signaling by IPv6 hop-by-hop options header and destination options header, which is suitable in the rapid changing environment and suitable for short lived and dynamic flows. It can also easily provide dynamic, fast adaptive to QoS situation changes and QoS requirements changes of real-time applications. The "Soft State" mode makes the resource reservation management simple and efficiently.

QoS aware handover for IP based ad hoc environments

Author : Yigang XU

Instructor : Matthias Riedel (SONY)

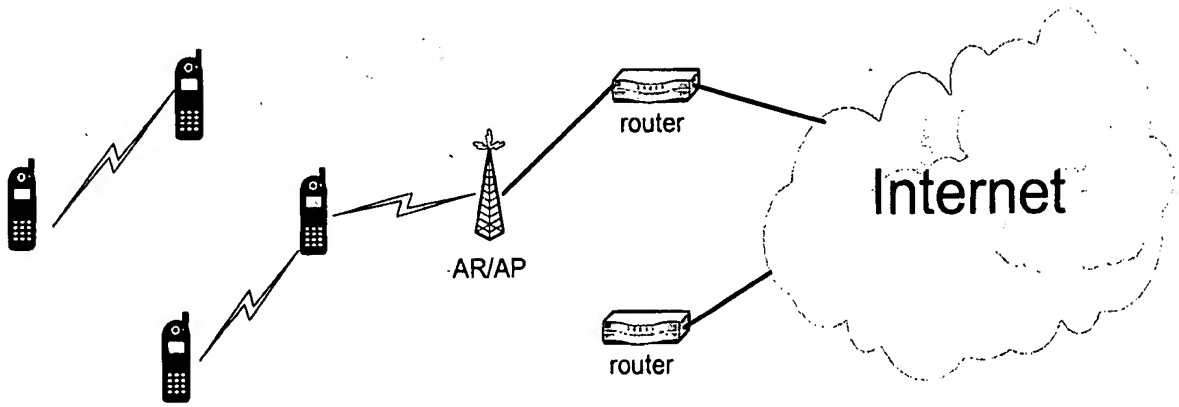
Content

- Design Analysis
  - Scope of the work
  - Future network architecture
  - Future application scenario
- Handover Issues
  - Introduction
  - Assumptions
- QoS-aware handover module in ASAP
  - Signaling and Procedures
  - "Local Recovery"
  - Comparison
- Conclusion and Future Works
- Appendix

Scope of the Invention

- We propose a QoS-aware handover module for ASAP QoS architecture, extending the network environment to wireless IPv6 access network with mobile ad hoc fringe.
- Our goal is to minimize the QoS degradation of adaptive real-time applications, due to the mobility of nodes in the above mobile, wireless network environment.
- We focus on real-time traffic flows, but the concept can still be applied to non real-time data.

Future All-IP based Mobile Network Architecture

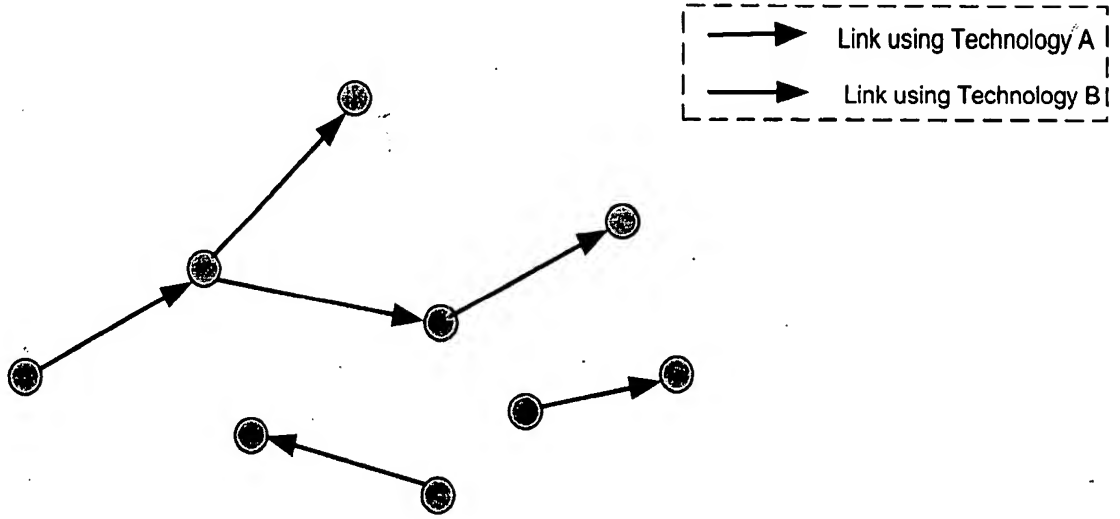


- Internet is still the basic of communication and data network, using IPv6.
- Mobile communication networks provide new services, forms access networks of the mobile internet.
- A strong trend of mobile ad hoc network solution.

Wireless Access Network

- Network architecture
  - Similar as fixed network
  - The last one hop is wireless connection
  - Mobility support is important
- QoS characteristics
  - Unstable wireless link leads to QoS variation for applications
  - Access part is the bottleneck, traffic crowded
  - Core part is resource over-provisioning
  - DiffServ / IntServ QoS model could be applied

Mobile Ad hoc Network (MANET)



- An autonomous distributed system of MNs
- The Union of MNs forms an arbitrary graph
- Dynamic, sometimes rapidly changing, random, multi-hop topologies
- Operate in a standalone fashion, or as a fringe network
- Bandwidth-constrained, variable capacity wireless links cause congestion frequently
- "Mobility" extends also into the realm of autonomous domain. No centralized administration, each node has to be configured on its own
- Power-constrained operation, relying on batteries for energy
- Limited physical security

Future Application Scenario

- All access technologies, wireless/wired link.
- All kinds of devices, wireless PDA, mobile phone, personal computer.
- All the time, stable/roaming, working on the road.
- All kinds of services, non-real time/real time/ adaptive real time applications.
- All traffics carried by IPv6 packets.

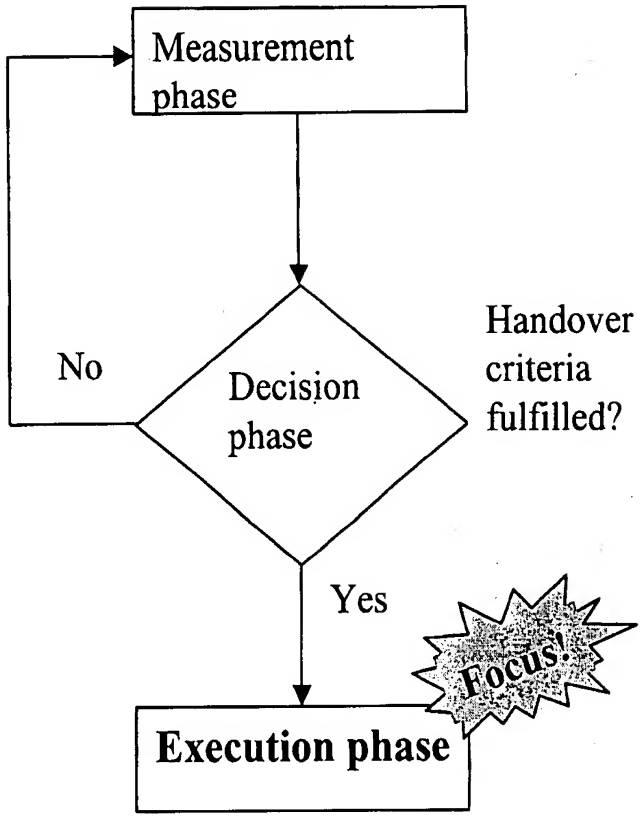
Problems?

- Most of proposals and fine-designed protocols consider the fixed network and mobile network separately, there are still many works to be done for the "Mobile Internet" world.
- QoS degradation caused
  - Ubiquitous mobility → Topology changes → Frequent rerouting → Delay and Packet loss expected over wireless links → QoS degrades frequently and substantially.
- QoS issues supporting for adaptive real time applications in wireless mobile IP network environment is at the early stage of research.
- Resource pre-allocation before handover occurs, is a good idea to satisfy QoS requirements of real time applications. This is the scope of our work.

Handover Issues

Introduction

- MNs are subject to changing their point of attachment from one access network to another. This process is called Handover.
- Handover triggers can be link-layer events (L2) or network-layer events (L3).
- Handover involves a change in link-layer connectivity, and sometimes in network-layer connectivity as well.
- The invention focuses on L3 handover execution phase.



Handover Phases.

Problems Caused by Handover

- Handover is the main obstacle of QoS support to real-time applications in wireless mobile IP network environment
  - Handover brings interruption to packet flows
  - Potential packets loss during handover procedure
  - No QoS or worse QoS support during or after handover procedure
- Handover procedure has a critical effect on the QoS architecture's operation

Seamless Handover – Wise Choice

- Handover module of QoS architecture should be deliberately selected and designed.
- Inefficient handover module could cause huge packet loss and long latency, make QoS recovery on the higher layer impossible.
- Seamless handover module is desired
  - Fast handover to avoid flow interruption, minimize packet loss.
  - Smooth handover to avoid packet lost.

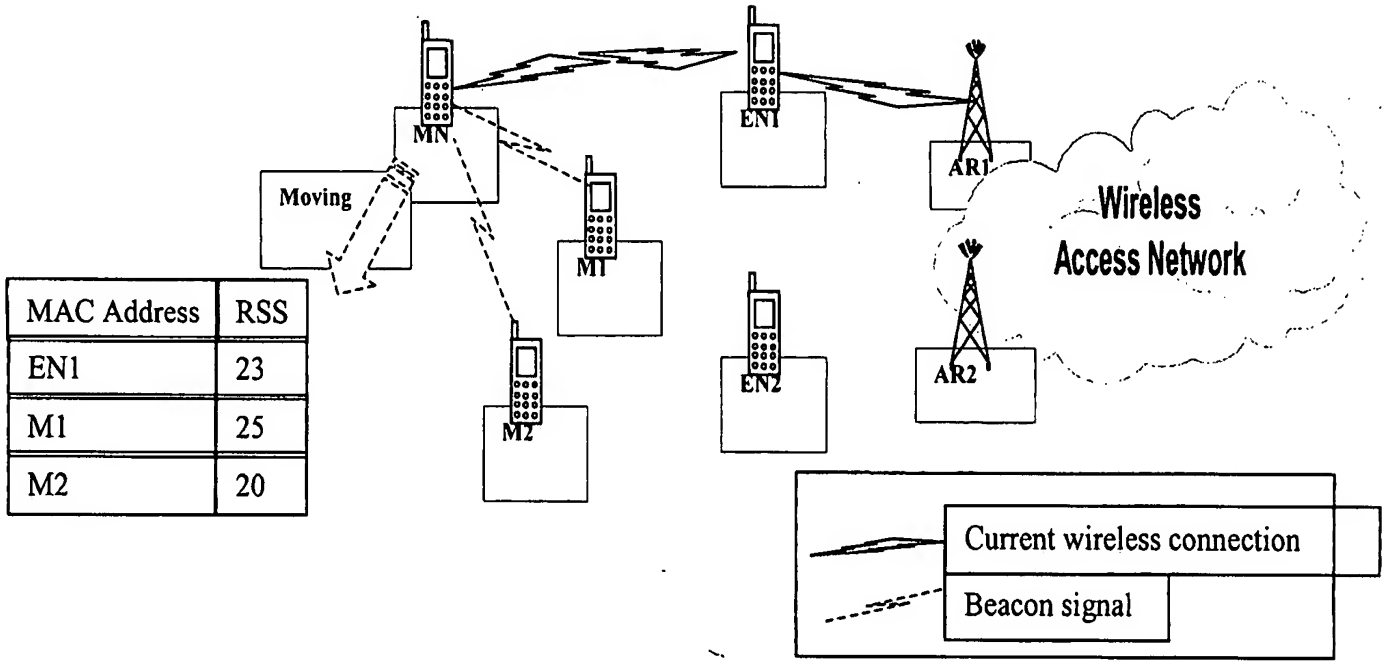
Assumptions

- Stable Issues
  - We focus on the scenario that MNs are roaming in the mobile ad hoc fringe, we assume the scalability is not the big problem to the handover module.
  - We don't specify any methods for detecting when the fringe partition occurs and when the partition heals.
  - We assume probed QoS metrics of wireless links are temporarily "stable" during the handover procedure.
- Reservation Issues
  - We assume that requests of resource reservation of wireless links, e.g. available bandwidth, could be processed and responded by lower layers.

QoS-aware Handover Module

--- Signaling and Procedures

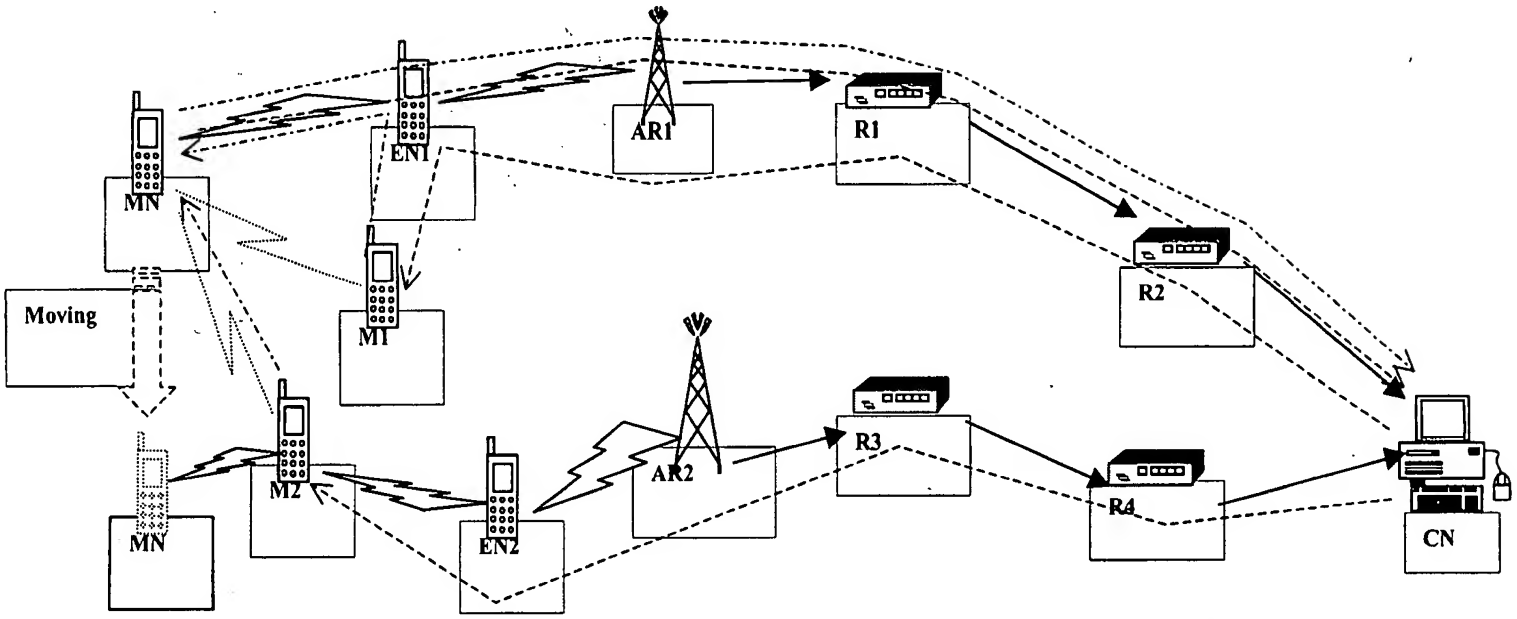
Candidate Nodes Finding



MAC Address	RSS
EN1	23
M1	25
M2	20

QoS-aware Handover Signaling of End Node

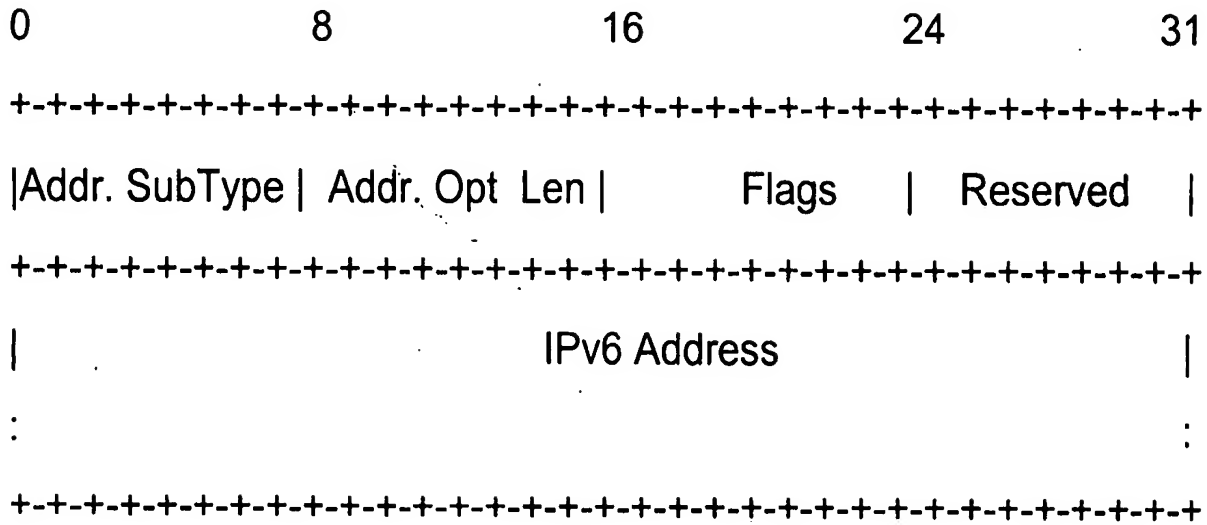
--- focus on MN which is source/sink node of the flow



1. Handover Initiation Signal (QoS metrics, target, candidates)
2. Handover QoS Metric Probing Signal (SR, QoS metrics, path history)
3. Handover QoS Metric Collection Signal (probed QoS metrics)
4. Handover Decision Signal (changed QoS metrics)
5. Handover Confirmation Signal (HR, QoS metrics)

MN: Mobile Node
M: Intermediate MN
EN: Egress Node
AR: Access Router
R: Intermediate Router
CN: Correspondent Node

ASAP IPv6 Address Option Data



Flags of IPv6 address type :

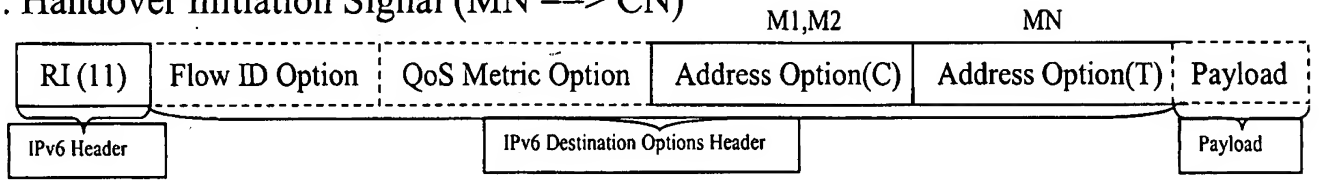
- Target node address (T)
- Candidate node address (C)
- Sending node address (S)

changed hop-by-hop for saving path history

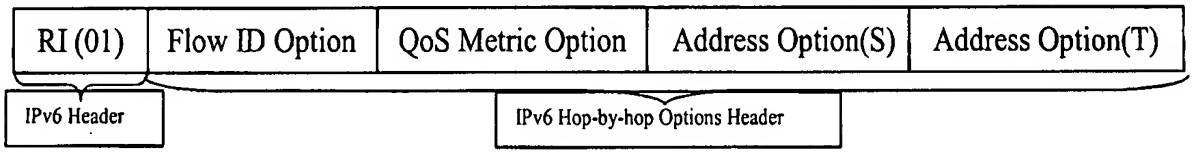
International (Europe) GmbH

QoS-aware Handover Signaling Format

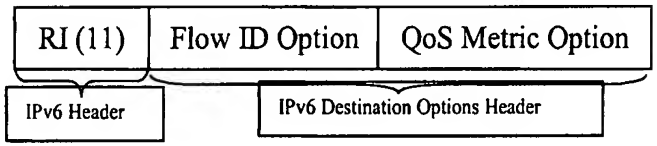
1. Handover Initiation Signal (MN ==> CN)



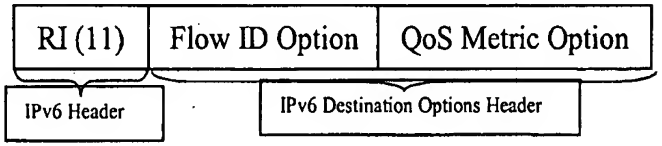
2. Handover QoS Metric Probing Signal (SR) (CN ==> M1,M2)



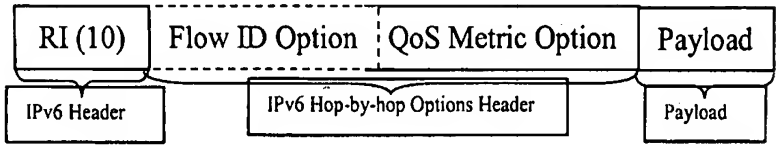
3. Handover QoS Metric Collection Signal (M1,M2 ==> MN)



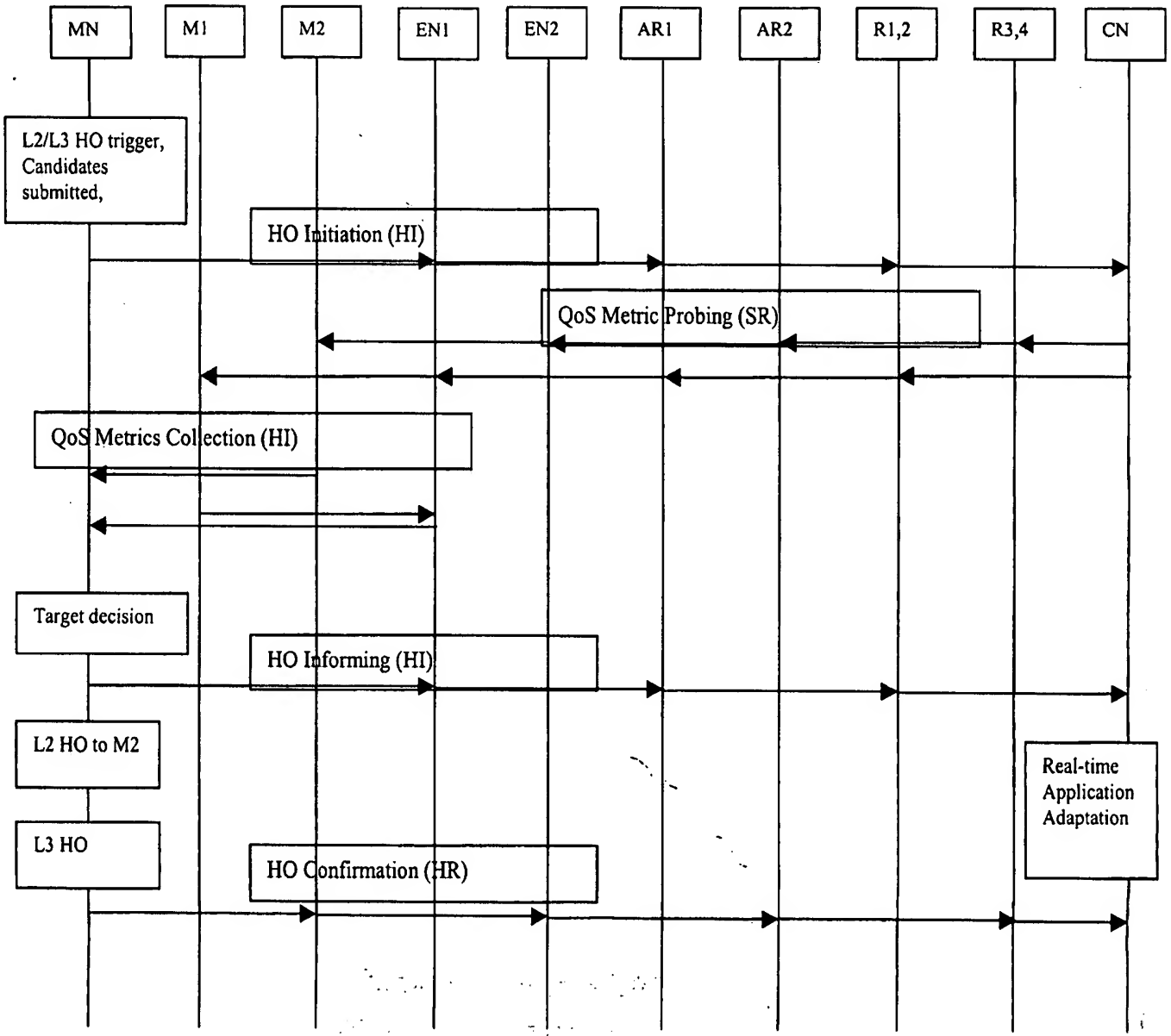
4. Handover Decision Signal (MN ==> CN)



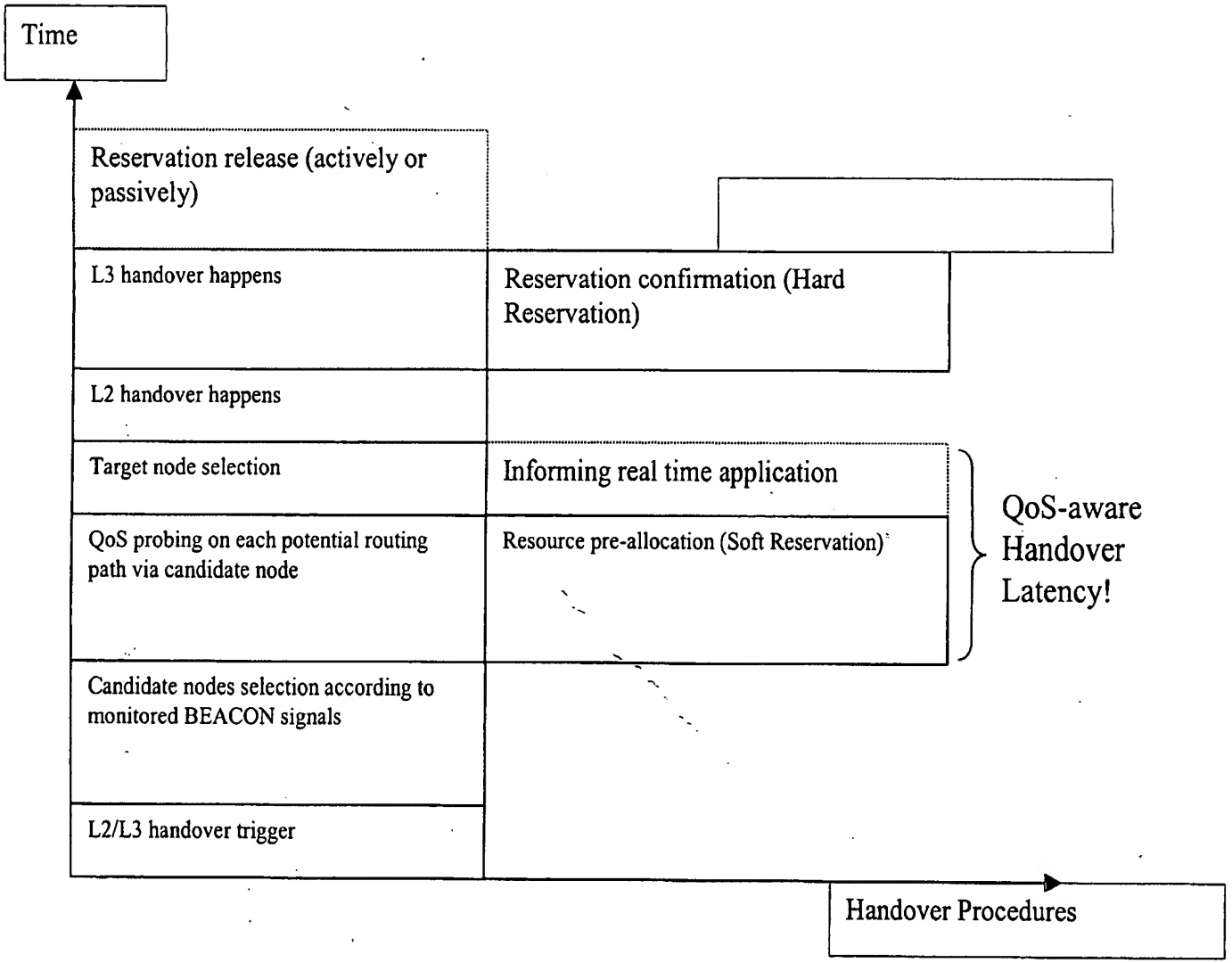
5. Handover Confirmation Signal (HR) (MN ==> M2 ==> CN)



Signaling for QoS-aware Handover

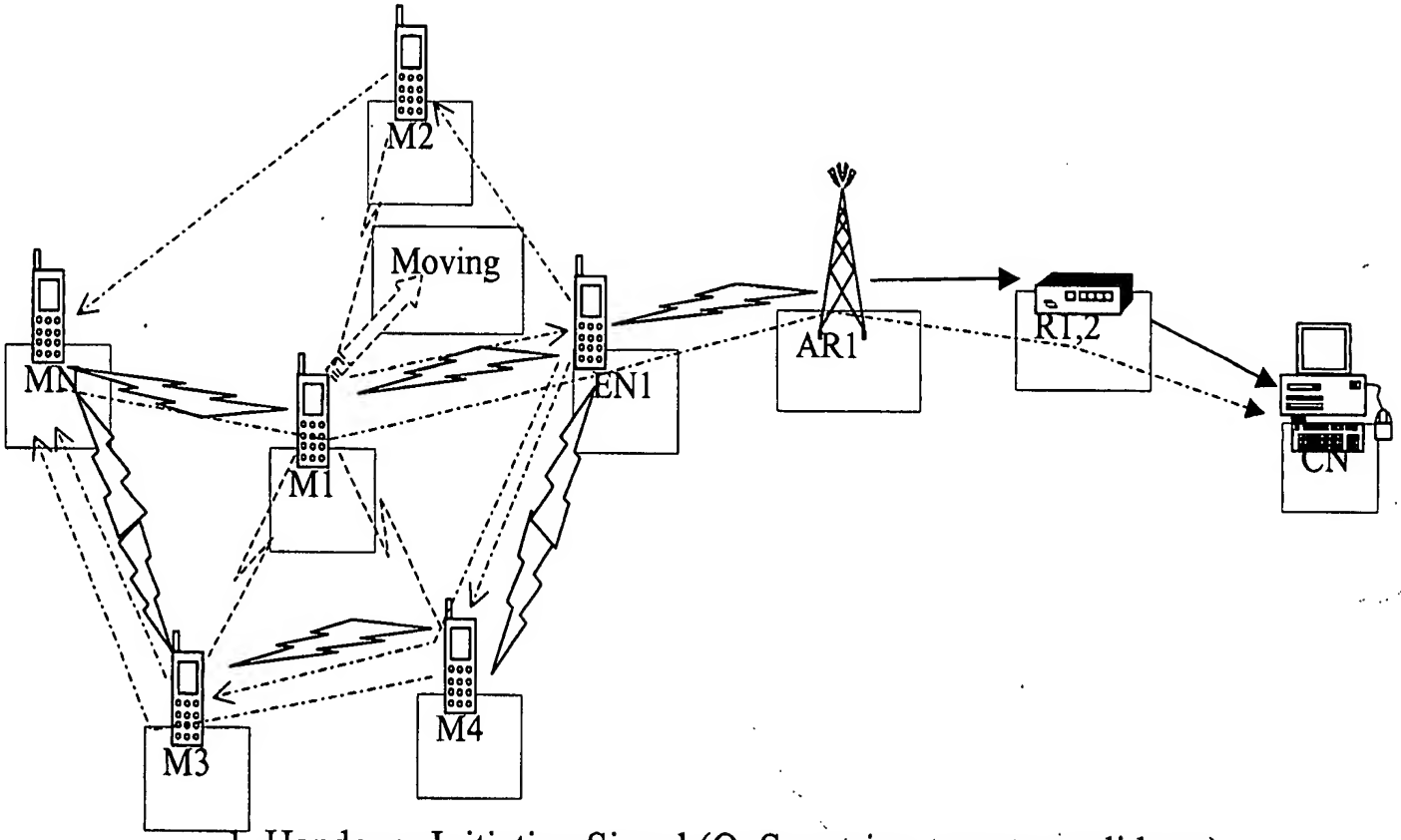


QoS-aware Handover Procedures



"Local Recovery" Signaling of Intermediate Node

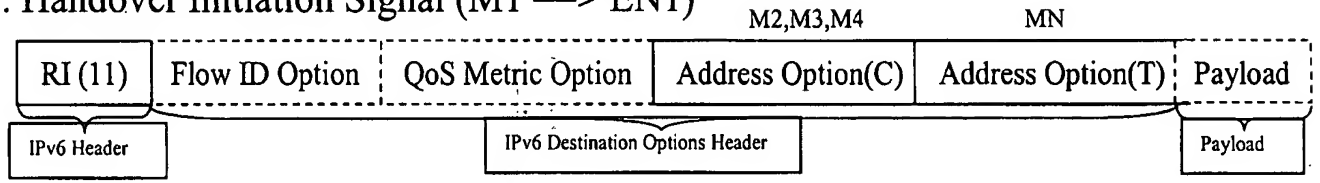
--- focus on MN which is hosting node of the flow



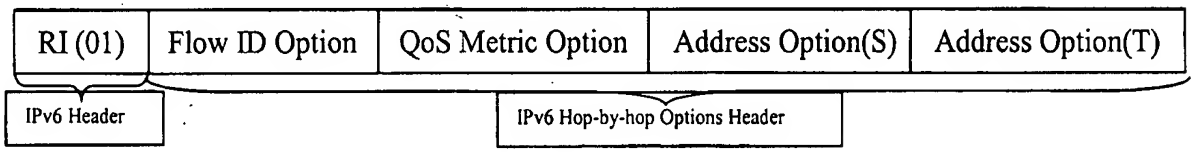
1. Handover Initiation Signal (QoS metrics, target, candidates)
2. Handover QoS Metric Probing Signal (SR, QoS metrics, path history)
3. Handover QoS Metric Collection Signal (probed QoS metrics)
4. Handover Decision Signal (changed QoS metrics)
5. Handover Confirmation Signal (HR, QoS metrics)

"Local Recovery" Signaling Format

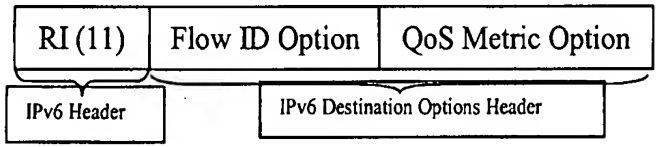
1. Handover Initiation Signal (M1 ==> EN1)



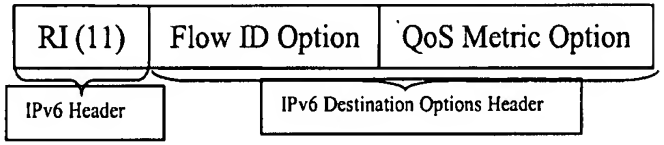
2. Handover QoS Metric Probing Signal (SR) (EN1 ==> M2,M3,M4)



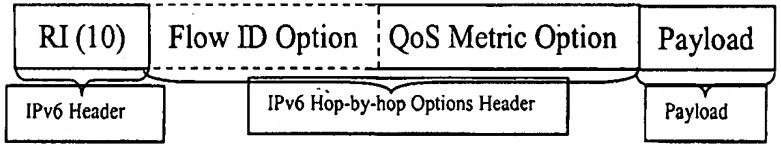
3. Handover QoS Metric Collection Signal (M2,M3,M4 ==> MN)



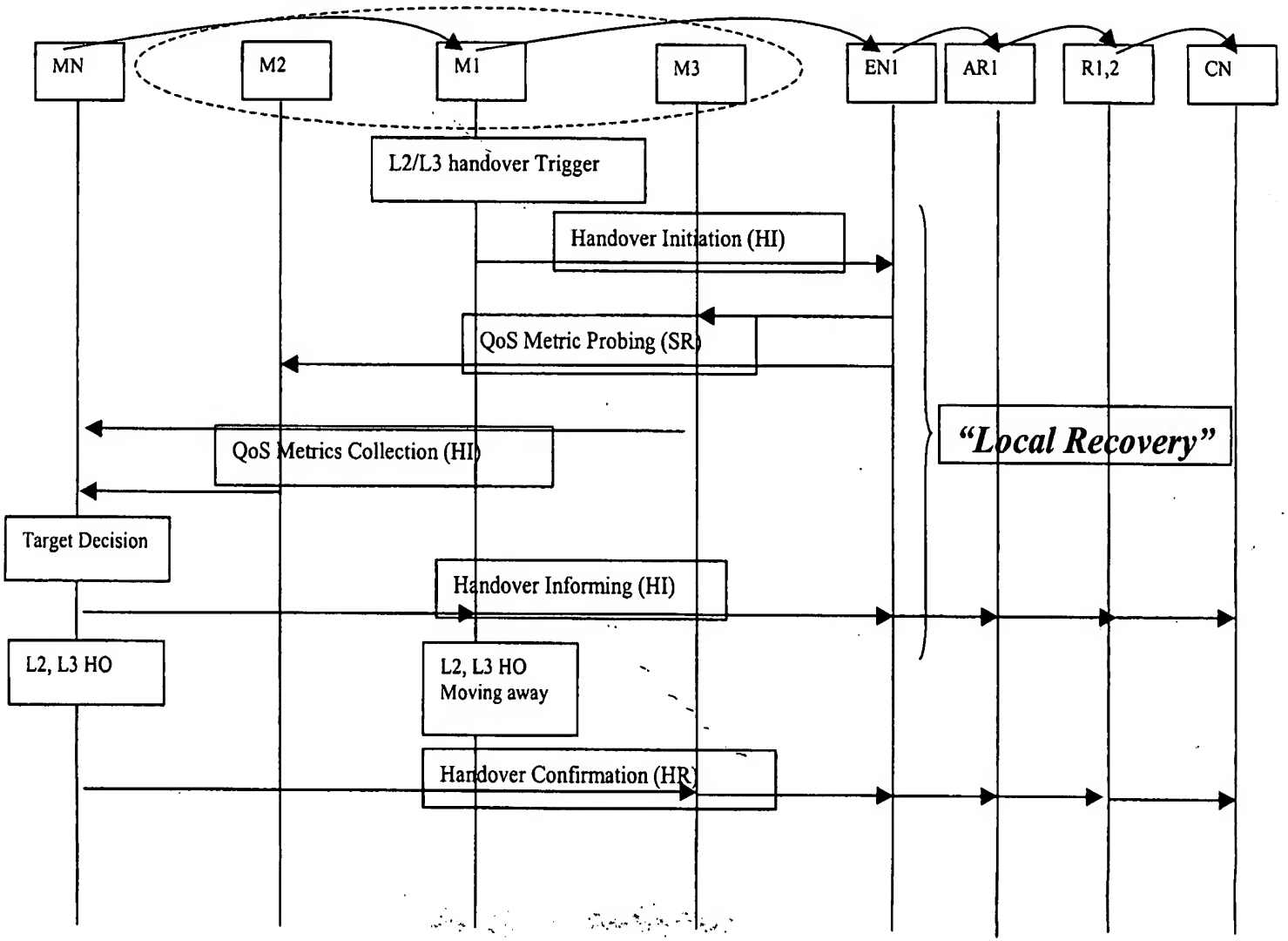
4. Handover Decision Signal (MN ==> CN)



5. Handover Confirmation Signal (HR) (MN ==> M3 ==> CN)



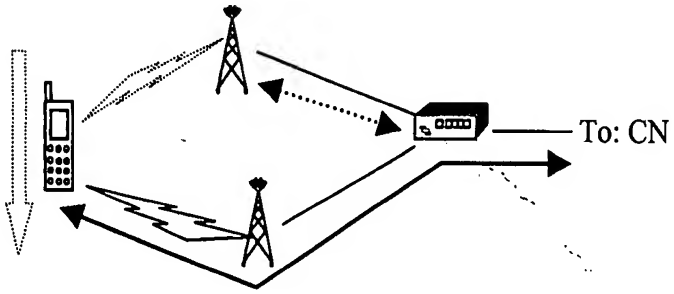
Signaling for "Local Recovery"



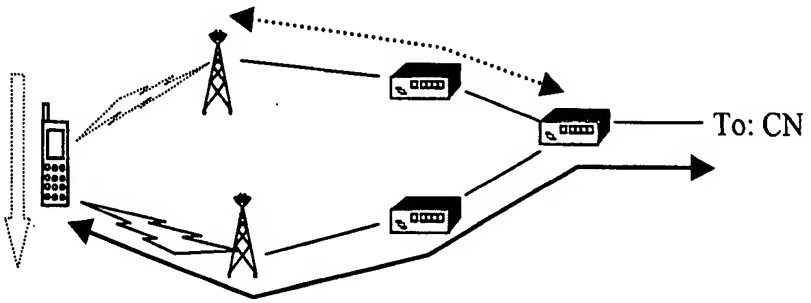
QoS-aware Handover Module

--- Comparison

RSVP Extensions



under Micro-Mobility



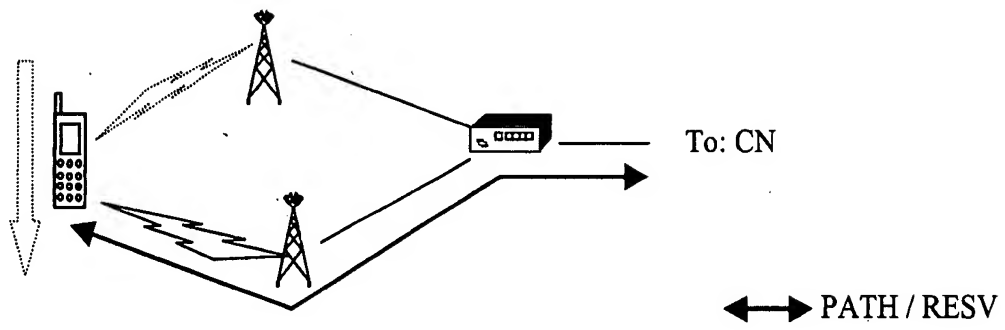
under Macro-Mobility

PATH / Active RESV

PATH / Passive RESV

- Active reservation on current path
- Passive reservation on potential paths, may be used temporarily by other connections
- After handover occurs, passive reservation is switched to active, and vice versa.
- "Advance Resource Reservation"
  - Increasing blocking rate of MN originating for RT flows
  - "Break-Before-Make" mode between BS and MN
  - An efficient partial path discovery mechanism is required, which is difficult
    - Caused inefficient resource reservation in advance
  - Overload for BS to maintain state information regarding Active/Passive reservations during handovers

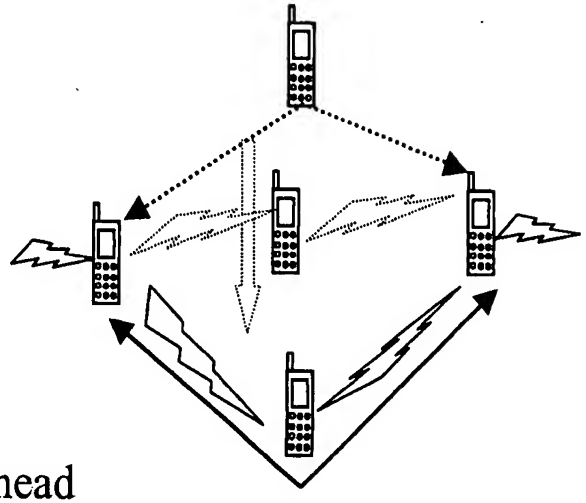
RSVP Standard



- "Local repair" provides fast adaptation to routing changes without the overhead of shorter refresh periods e.g., reducing the soft state timer.
  - The local routing protocol module notify RSVP process of route changes for particular destinations.
  - RSVP use this information to trigger PATH/RESV refreshes for these destinations, using the new route.
- "Break-Before-Make" mode
- RSVP signaling overhead in mobile environment,
  - longer resource reservation delay
  - greater number of packets loss

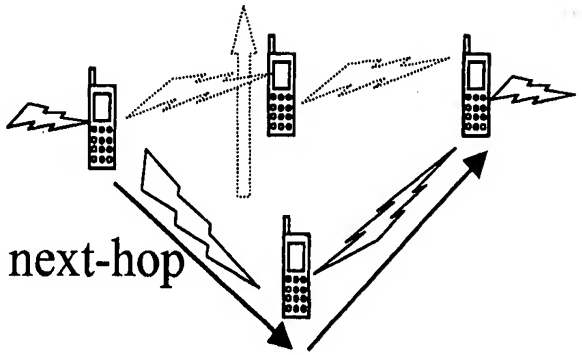
QoS-aware Handover with "Local Recovery"

- End-to-End QoS-aware handover
  - + Independent of mobility management
  - + Resource reserved on the right path between MN and CN, which is optimized by the routing protocol
  - + Can be also used for path setup originating for RT flows
  - -- Long round-trip resource reserved delay
  - -- Large signaling overhead caused by end-to-end negotiation
- "Local Recovery"
  - Resource Pre-allocation
    - Soft state
  - Make-Before-Break
    - No packets loss
  - Fast adaptation
    - Limiting process of negotiation
    - Minimizing delay and signaling overhead



INSIGNIA

- Adaptive QoS Support in MANETs
  - In-band signaling
    - Responsive enough to network conditions, e.g., frequent rerouting
    - Fast resource reservation
    - Timely adaptive
  - Soft state
    - Outstanding management and maintenance of resource reservations
    - States automatically time out



- Rerouting and Restoration
  - "Break-before-Make" mode
  - Based on the routing protocol to find next-hop
  - Immediate flow restoration
  - Service maybe downgraded, no guarantee

Conclusion (1)

QoS-aware handover procedure and QoS monitoring procedure in ASAP are integrated into a simple, compact QoS control architecture.

- Simple and efficient in implementation.
  - Using IPv6 hop-by-hop and destination options header
  - Minimize the signaling and processing load.
- QoS monitoring procedure
  - Using In-band signaling
    - Suitable in the rapid changing environment
    - Suitable for short lived and dynamic flows
  - Dynamic, fast adaptive
    - QoS situation changes
    - QoS requirements of real time applications
  - Soft state
    - Efficient resource reservation

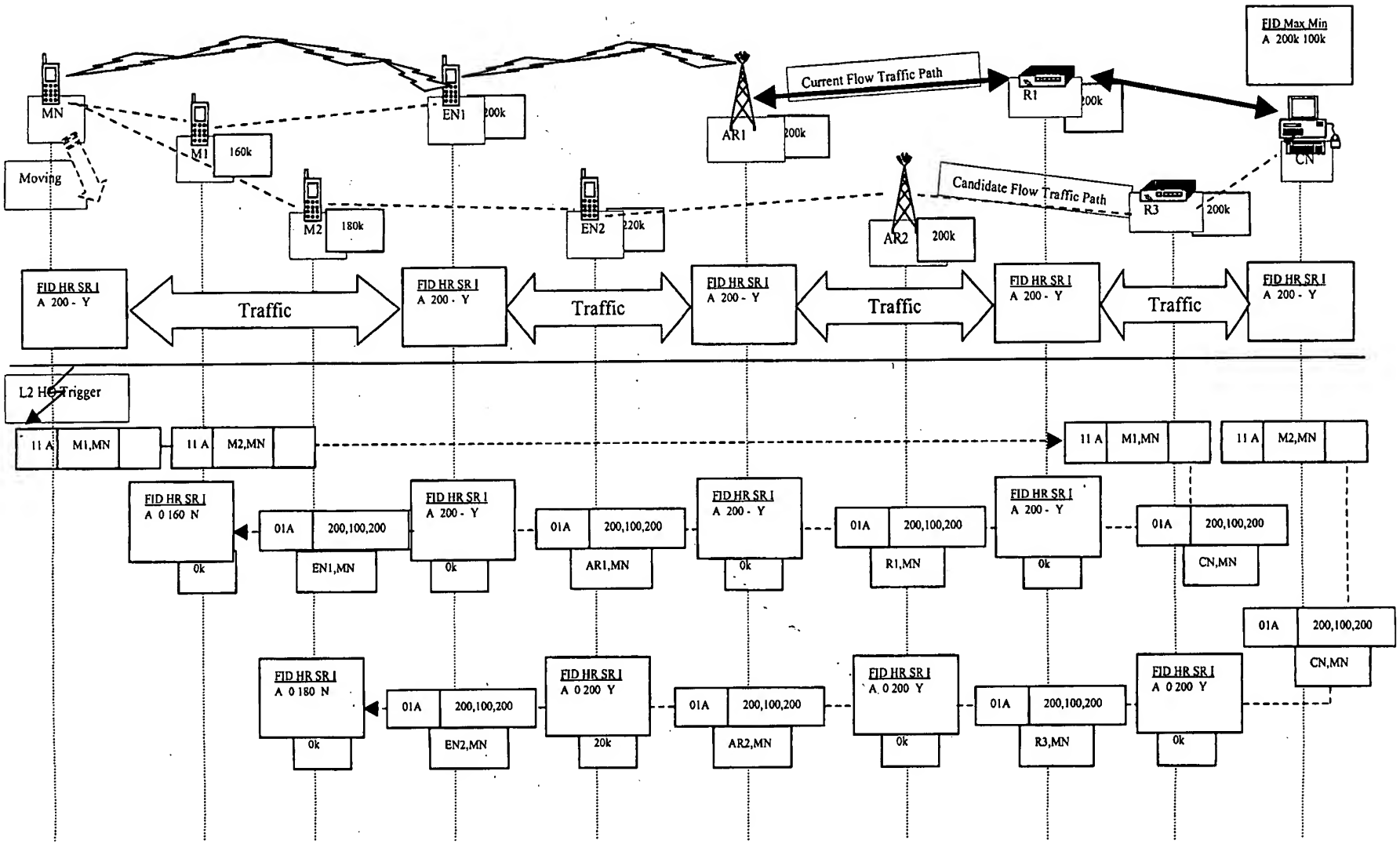
Conclusion (2)

- QoS-aware handover module
  - L3 handover, independent of any L2 radio access technologies.
  - Independent of any particular mobility management.
  - Seamless handover, much of the information can be "anticipated" collected in advance of L2/L3 handover.
  - Using "MIAMI", automatically and dynamically identify neighbors without much administrative intervention.
  - "Pre-allocation", providing candidates' IPv6 addresses along with their capabilities for target handover node selection.
  - "Local Recovery" adapts to changes in network topology and resource availability, reactive to QoS violations.

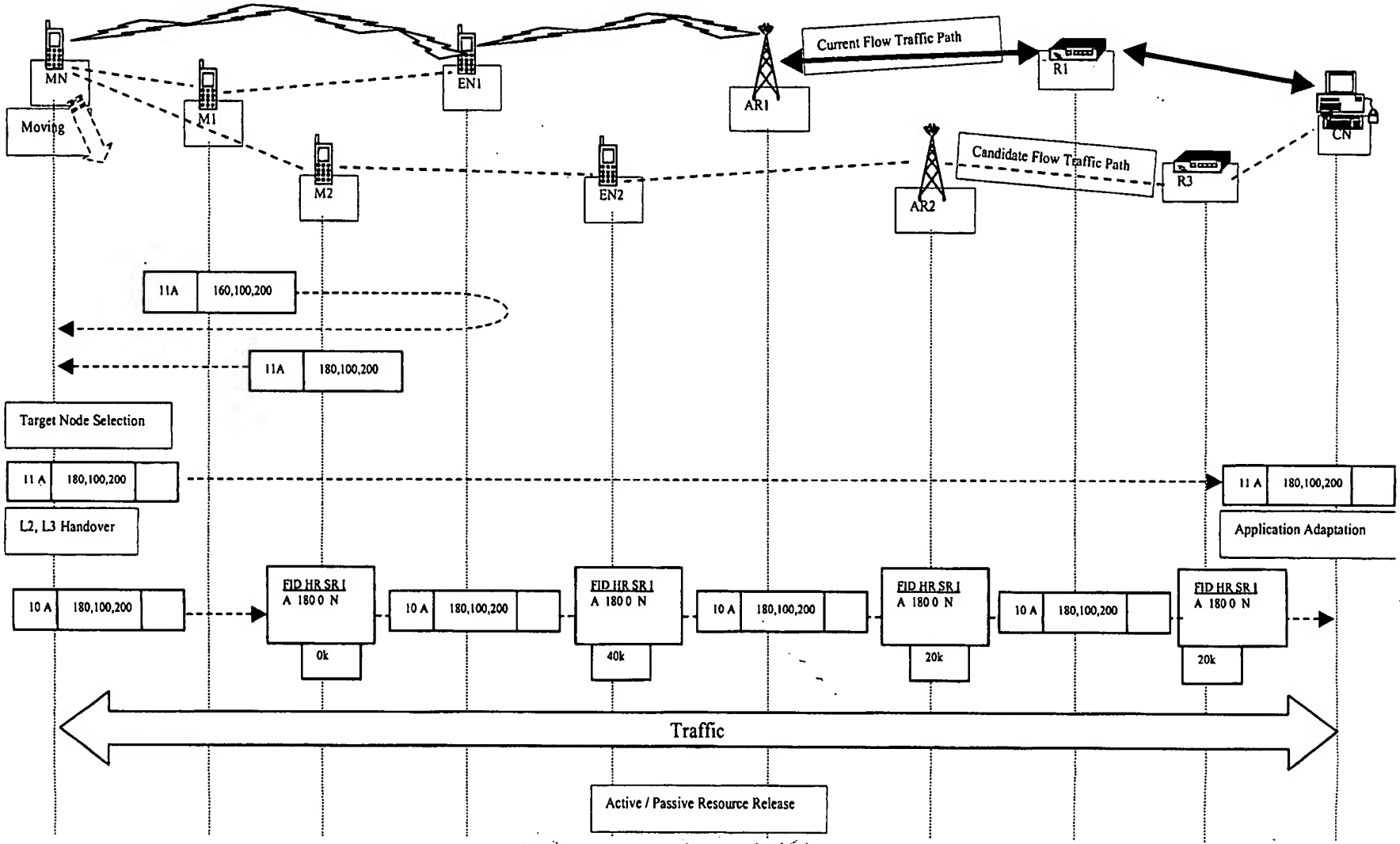
Future works

- The following works should be done in order to refine this QoS-aware handover module and further support ASAP QoS model:
  - Movement prediction will be helpful for efficient candidates selection, resource pre-allocation. This is more like a mathematic question.
  - "Traffic Control" module of the kernel will be helpful for resource reservation implementation.
  - To limit the handover negotiation, minimize delay and signalling overheads with the help of mobility management.
  - Context Transfer support.
  - Security and robust consideration.

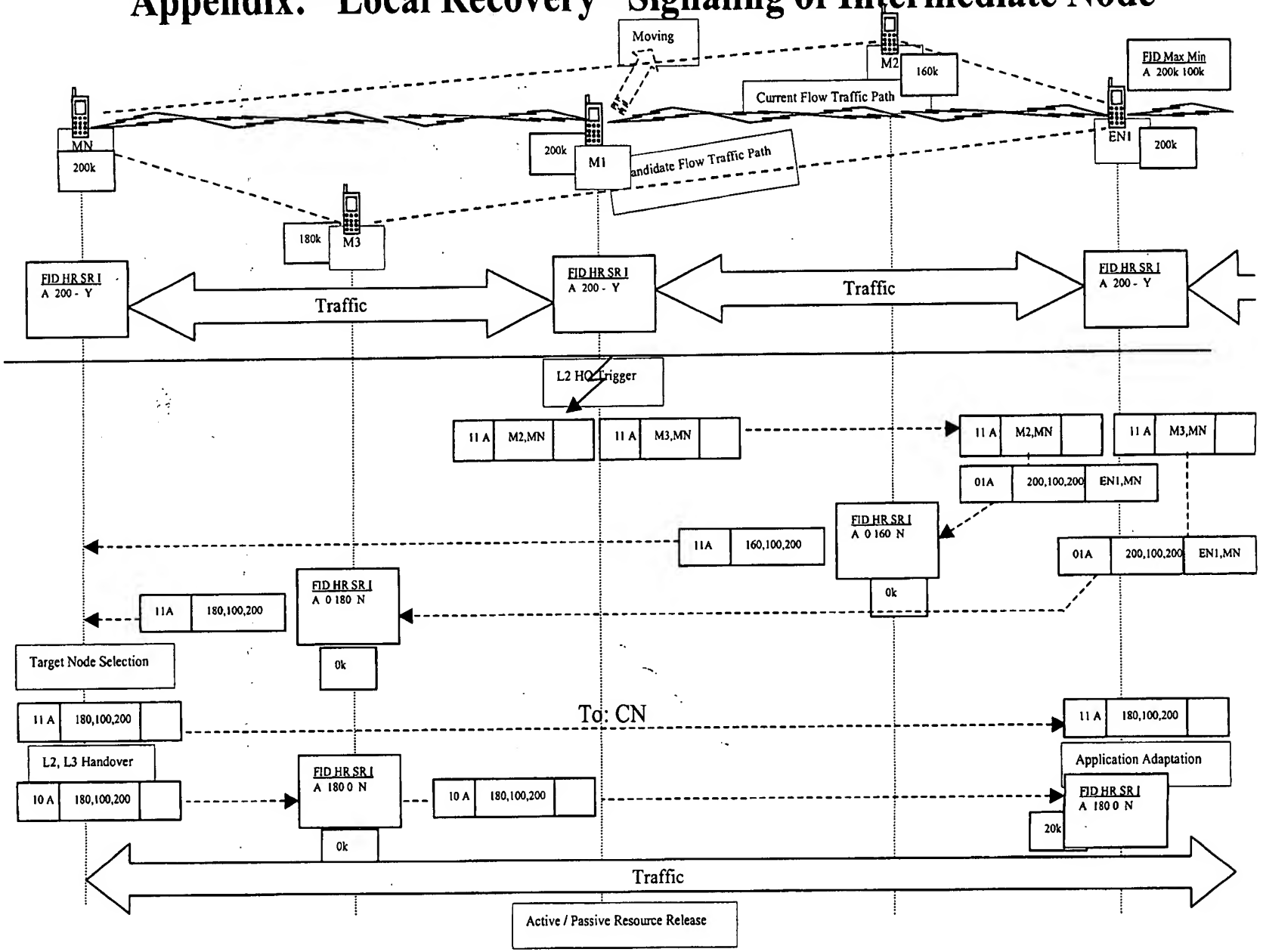
Appendix: QoS-aware Handover Signaling of End Node (1)



Appendix: QoS-aware Handover Signaling of End Node (2)

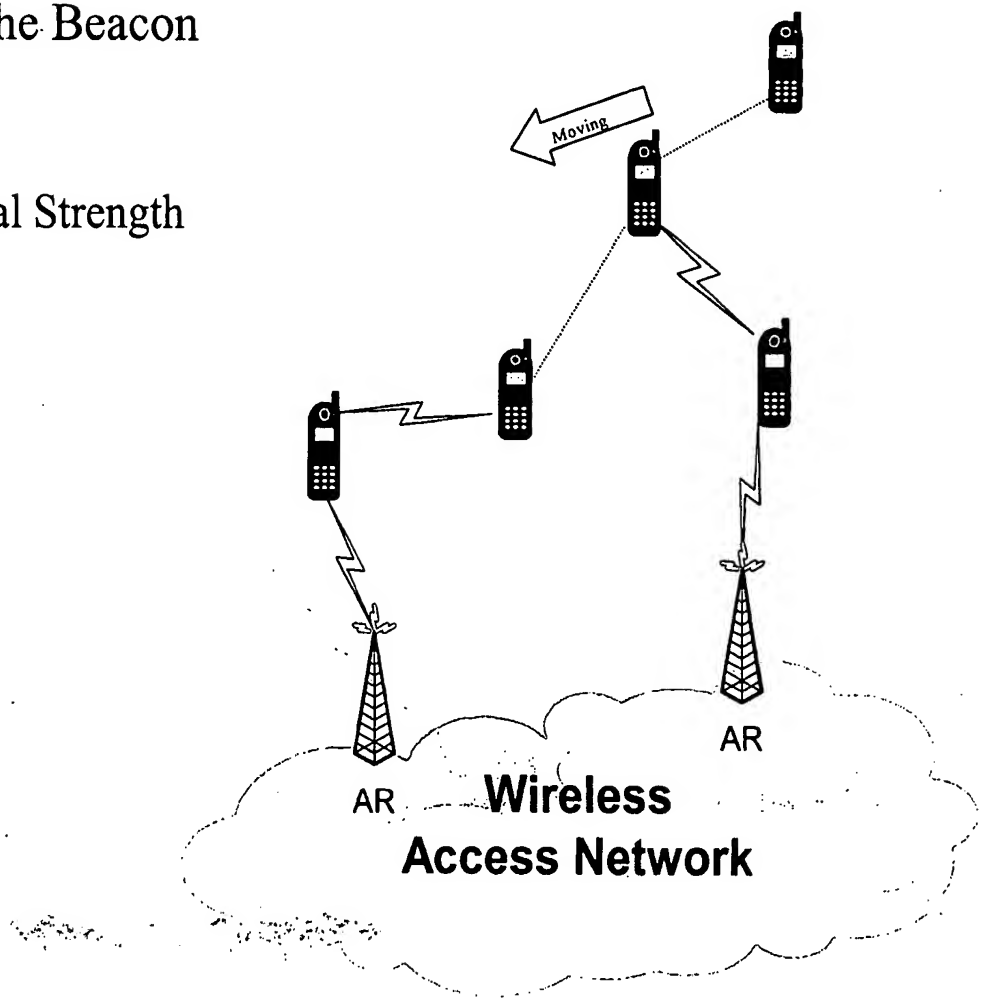


Appendix: "Local Recovery" Signaling of Intermediate Node



Motivation

- We assume that the Beacon signal includes:
  - MAC address
  - Received Signal Strength (RSS)



International (Europe) GmbH

MAC-IP Address Mapping Implementation (MIAMI)

Author : Yigang XU

Instructor : Matthias Riedel (SONY)

Sony International (Europe) GmbH
P.27925EP

EPO - Munich
50
10. März 2003

„QoS aware handover"

Claims:

1. A method for handover in Intenet Protocol based ad-hoc networks, the handover step being carried out QoS-aware.

2. A method according to claim 1,
   characterized by the steps of
   resource probing, pre-allocating, reserving, and adapting in the dynamic ad hoc environment.

3. A cellular telecommunications network with QoS aware handover functionality.

4. A cellular telecommunications network with QoS aware handover functionality according to claims 1 or 2.

5. A mobile base station designed for implementing a method according to claim 1.

THIS PAGE BLANK (USPTO)

Existing Approaches for Address Resolution (2)

- IPv6 Neighbor Discovery Protocol (ND)
  - Extending and improving on IPv4's ARP
  - Embedded within ICMPv6
  - Defining new functionality, Neighbor Unreachability Detection
  - Need of multicast-capable interface
  - Performed only on addresses that are determined to be on-link, never on multicast addresses
  - Unsolicited node doesn't need to create an entry in the cache when receiving a valid Neighbor Advertisement
- Inverse Neighbor Discovery Protocol (IND)
  - Extensions to IPv6 ND
  - Developed for Frame Relay networks, or networks with similar behavior
  - IND Solicitation is sent as IPv6 all-node multicast. However at link layer, it is sent directly to the target node, a directly connected remote node identified by the known link-layer address.

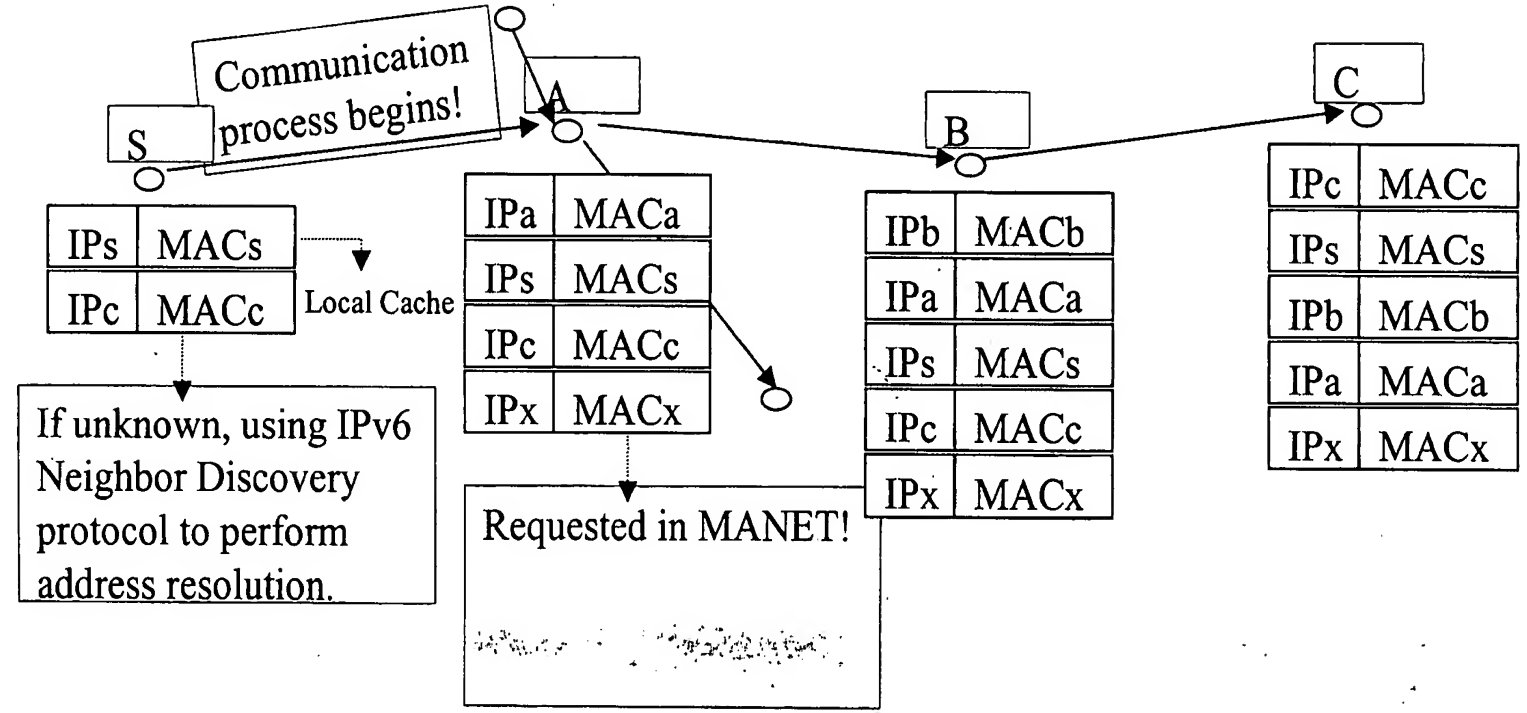
Existing Approaches for Address Resolution (1)

- ARP in IPv4
  - Useful in a broadcast medium, like Ethernet
  - Using flooding packets
  - Every host has a small cache to save mapping information
  - All hosts are equal in status, no distinction between clients and servers.
- Reverse ARP (RARP)
  - Also used in broadcast medium with flooding packets
  - Need one or more server hosts
    - to maintain a database of mapping information,
    - to respond to requests from client hosts.
  - Most implementations will require some form of interaction with a program outside of the kernel
  - Separate protocol at the data-link level, different from ARP
    - Medium independent
    - Can be used for mapping hardware addresses to any higher level protocol address

Description of MIAMI

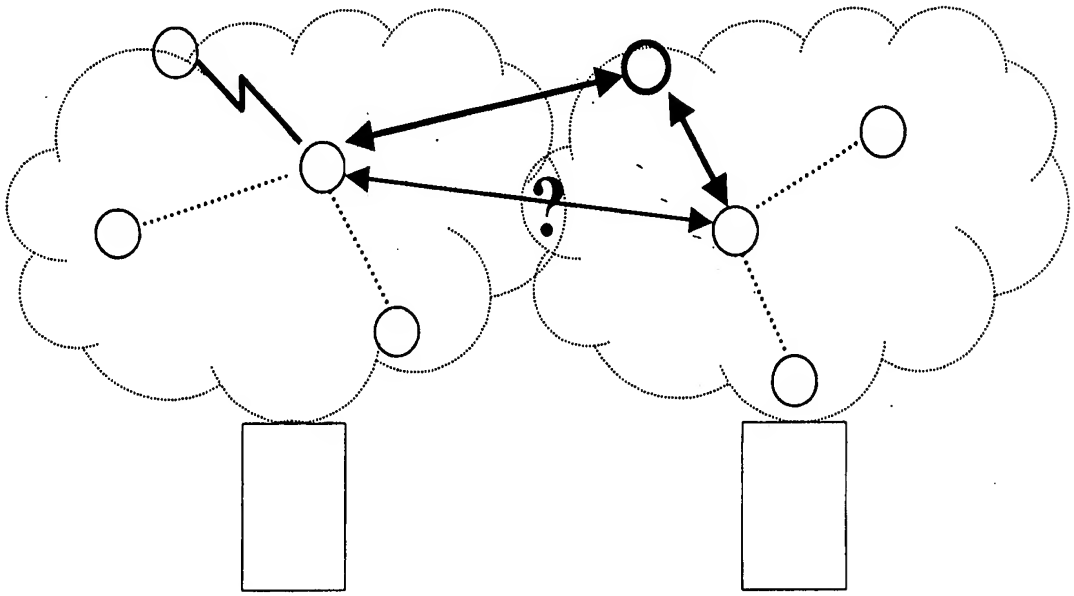
- Using IPv6 hop-by-hop options header to propagate mapping information.
- Flags: Media Type, Network Prefix information, or others.

	Opt Type	Opt Len
Flags	Lifetime	
MAC address (48 bits)		
IPv6 address		



MAC-IP Address Mapping Implementation (MIAMI)

- Problems for ND/IND in MANETs
  - Packets loss during ND/IND procedures because of broken link
  - Packets loss makes multicast communication even worse
  - limits of simultaneous connectivity
- "Information Dissemination" is important in MANETs
  - Data replication, increasing availability of mapping information
  - Minimizing usage of ND/IND, lower communication overhead
  - MN without multicast-capable interface can also resolve addresses
  - Multiple technologies can be utilized



Characteristics of MIAMI

- An approach for "Information Dissemination"
- Not a "really" address resolution protocol
- Supports to address resolution (MAC <=> IP) in MANETs
- Using MIAMI packets missing MAC or IPv6 address field in the options header, to actively propagate "Requests"
  - "Soft", smooth operation
  - Unlike "hard" IPv6 ND/IND
- Supplement to IPv6 ND/IND
  - "Simple, lightweight" design, without much administrative intervention
  - No central server/agent needed
  - "Proactively" propagating address mapping information
  - Minimize the need of IPv6 ND/IND
  - Interaction with local cache, e.g. Neighbor Discovery Cache
    - Actively expand cached information
    - Frequently update
    - Suitable to dynamic network environment
- An automatic, distributed and dynamic mechanism

THIS PAGE BLANK (USPTO)

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.